National Critical Information Infrastructure Protection Centre

CVE Report

01st Oct- 15th Oct 2016 **Vol. 03 No. 17**

Vulnerability Type(s)	Publish Date	CVSS	Description CVE ID	Patch	NCIIPC ID
Application (A)					
Adobe					
Acrobat; Acrobat Dc; Acrobat Reader Dc; Reader Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents. Acrobat DC and Acrobat Reader DC are the successors to Adobe Acrobat 11 and Adobe Reader 11.					
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/01

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7017**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/02

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7016**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/03

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7015**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/04

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7014**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/05

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7013**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/06

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7012**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/07

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7011**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/08

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7010**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/09

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7009**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/10

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7008**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/11

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7007**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/12

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7006**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/13

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7005**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/14

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7004**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/15

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7003**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/16

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7002**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/17

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7001**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/18

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-7000**		
Execute Code; Overflow	2016-10-14	10	Integer overflow in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-6999**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/19
Denial of	2016-10-14	10	Adobe Reader and Acrobat	https://helpx	A-ADO-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Service; Execute Code Overflow; Memory Corruption			before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6998**	.adobe.com/security/products/acrobat/apsb16-33.html	ACROB--201016/20

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/21

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6997		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/22

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-6996		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/23

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			7018, and CVE-2016-7019. **Reference: CVE-2016-6995**		
Execute Code; Overflow	2016-10-14	10	Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-6939. **Reference: CVE-2016-6994**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/24
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, and	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/25

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			CVE-2016-6988. **Reference: CVE-2016-6993**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, and CVE-2016-6993. **Reference: CVE-2016-6988**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/26
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/27

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6979**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/28

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6978**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6978, CVE-2016-6995, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/29

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6977**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6977, CVE-2016-6978, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/30

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6976**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6976, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/31

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6975**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6975, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/32

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6974**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/33

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6973**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/34

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6972**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/35

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6971**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/36

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6970**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6969**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/37
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/38

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6968**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/39

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			CVE-2016-6993. **Reference: CVE-2016-6967**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/40

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6966**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6965**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/41
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/42

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6964**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6963**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/43

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6962**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/44
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/45

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6961**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/46

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6960**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/47

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6959**		
Bypass	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to bypass intended access restrictions via unspecified vectors. **Reference: CVE-2016-6958**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/48
Bypass	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors. **Reference: CVE-2016-6957**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/49
Denial of Service; Execute Code Overflow; Memory	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and	https://helpx.adobe.com/security/products/acrobat	A-ADO-ACROB--201016/50

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Corruption			Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6956**	/apsb16-33.html	
Denial of Service; Execute Code Overflow;	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic	https://helpx.adobe.com/security/prod	A-ADO-ACROB--201016/51

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Memory Corruption			before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6955**	ucts/acrobat/apsb16-33.html	
Denial of Service; Execute	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and	https://helpx.adobe.com/s	A-ADO-ACROB--

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Code Overflow; Memory Corruption			Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6954**	ecurity/products/acrobat/apsb16-33.html	201016/52
Execute Code	2016-10-14	10	Use-after-free vulnerability	https://helpx	A-ADO-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6953**	.adobe.com/security/products/acrobat/apsb16-33.html	ACROB--201016/53
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/54

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6952**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/55

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6951**		
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/56

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6950**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6949**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/57
Denial of Service; Execute Code	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic	https://helpx.adobe.com/security/prod	A-ADO-ACROB--201016/58

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Overflow; Memory Corruption			before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6948**	ucts/acrobat/apsb16-33.html	
Denial of Service;	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and	https://helpx.adobe.com/s	A-ADO-ACROB--

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Execute Code Overflow; Memory Corruption			Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6947**	ecurity/products/acrobat/apsb16-33.html	201016/59
Execute Code	2016-10-14	10	Use-after-free vulnerability	https://helpx	A-ADO-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6946**	.adobe.com/security/products/acrobat/apsb16-33.html	ACROB--201016/60
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/61

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6945**		
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-6944**	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/62
Denial of Service; Execute Code Overflow; Memory	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader	https://helpx.adobe.com/security/products/acrobat/apsb16-	A-ADO-ACROB--201016/63

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Corruption			DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6943**	33.html	
Denial of Service; Execute Code Overflow;	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and	https://helpx.adobe.com/security/products/acrobat	A-ADO-ACROB--201016/64

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Memory Corruption			Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6942**	/apsb16-33.html	
Denial of Service; Execute Code	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic	https://helpx.adobe.com/security/prod	A-ADO-ACROB--201016/65

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Overflow; Memory Corruption			before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6941**	ucts/acrobat/apsb16-33.html	
Denial of Service; Execute	2016-10-14	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and	https://helpx.adobe.com/s	A-ADO-ACROB--

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Code Overflow; Memory Corruption			Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019. **Reference: CVE-2016-6940**	ecurity/products/acrobat/apsb16-33.html	201016/66
Execute Code	2016-10-14	10	Use-after-free vulnerability	https://helpx	A-ADO-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-1091**	.adobe.com/security/products/acrobat/apsb16-33.html	ACROB--201016/67
Execute Code	2016-10-14	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--201016/68

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993. **Reference: CVE-2016-1089**		
Flash Player Adobe Flash Player is the standard for delivering high-impact, rich Web content. Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.					
Execute Code	2016-10-06	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-7020**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH--201016/69
Flash Player; Flash Player Desktop Runtime Adobe Flash Player is the standard for delivering high-impact, rich Web content. Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.					
Bypass	2016-10-14	10	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on	https://helpx.adobe.com/security/products/flash-player/apsb1	A-ADO-FLASH--201016/70

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Linux allows attackers to bypass intended access restrictions via unspecified vectors. **Reference: CVE-2016-4286**	6-32.html	
Ajax-random-post Project					
Ajax-random-post Random Post with Ajax includes Choice Categories, Choice of Post Type, Possibility to choose the number of posts, Display post date, Show Thumbnail of post, Beautiful design, User friendly and Responsive features.					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin ajax-random-post v2.00. **Reference: CVE-2016-1000127**	NA	A-AJA-AJAX---201016/71
American Auto-matrix					
Aspect-matrix Building Automation Front-end Solutions Application; Aspect-nexus Building Automation Front-end Solutions Application Building Automation Front-end Solutions provide Integration and Energy Control Solution designed to provide users seamless access to their building data through common and convenient web technologies available on the devices.					
Gain Information	2016-10-05	7.5	American Auto-Matrix Aspect-Nexus Building Automation Front-End Solutions application before 3.0.0 and Aspect-Matrix Building Automation Front-End Solutions application store passwords in cleartext, which allows remote attackers to obtain sensitive information by reading a file. **Reference: CVE-2016-2308**	https://ics-cert.us-cert.gov/advisories/ICSA-16-273-01-0	A-AME-ASPEC--201016/72
Gain Information	2016-10-05	5	American Auto-Matrix Aspect-Nexus Building Automation Front-End Solutions application before 3.0.0 and Aspect-Matrix Building Automation Front-End Solutions application	https://ics-cert.us-cert.gov/advisories/ICSA-16-273-01-0	A-AME-ASPEC--201016/73

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			allow remote attackers to read arbitrary files via unspecified vectors, as demonstrated by the configuration file. **Reference: CVE-2016-2307**		
Anti-plagiarism Project					
Anti-plagiarism Anti-plagiarism tool cannot scan printed offline sources but the publications that are online are available. Plagiarism checker free download is the simplest and the cheapest solution of a "copy-paste" problem. This unique program is an advanced expert in writing fraud detection.					
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin anti-plagiarism v3.60 **Reference: CVE-2016-1000128**		A-ANT-ANTI---201016/74
Apache					
Derby Apache Derby (previously distributed as IBM Cloudscape) is a relational database management system (RDBMS) developed by the Apache Software Foundation that can be embedded in Java programs and used for online transaction processing.					
Denial of Service	2016-10-04	6.4	XML external entity (XXE) vulnerability in the SqlXmlUtil code in Apache Derby before 10.12.1.1, when a Java Security Manager is not in place, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via vectors involving XmlVTI and the XML datatype. **Reference: CVE-2015-1832**	https://svn.apache.org/viewvc?view=revision&revision=1691461	A-APA-DERBY--201016/75
Myfaces Apache MyFaces is an Apache Software Foundation project that creates and maintains an open-source JavaServer Faces implementation, along with several libraries of JSF components that can be deployed on the core implementation. Apache MyFaces is an Apache Software Foundation project that creates and maintains an open-source JavaServer Faces implementation, along with several libraries of JSF components that can be deployed on the core implementation.					
NA	2016-10-06	7.5	CoreResponseStateManager	https://issues	A-APA-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			in Apache MyFaces Trinidad 1.0.0 through 1.0.13, 1.2.x before 1.2.15, 2.0.x before 2.0.2, and 2.1.x before 2.1.2 might allow attackers to conduct deserialization attacks via a crafted serialized view state string. **Reference: CVE-2016-5019**	.apache.org/jira/browse/TRINIDAD-2542	MYFAC--201016/76
Struts Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model–view–controller (MVC) architecture.					
NA	2016-10-04	7.5	Apache Struts 2 before 2.3.29 and 2.5.x before 2.5.1 allow attackers to have unspecified impact via vectors related to improper action name clean up. **Reference: CVE-2016-4436**	https://struts.apache.org/docs/s2-035.html	A-APA-STRUT--201016/77
Tomcat Tomcat, is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF). Tomcat implements several Java EE specifications including Java Servlet, JavaServer Pages (JSP), Java EL, and WebSocket, and provides a "pure Java" HTTP web server environment in which Java code can run.					
Gain Privileges	2016-10-03	7.2	The Tomcat init script in the tomcat7 package before 7.0.56-3+deb8u4 and tomcat8 package before 8.0.14-1+deb8u3 on Debian jessie and the tomcat6 and libtomcat6-java packages before 6.0.35-1ubuntu3.8 on Ubuntu 12.04 LTS, the tomcat7 and libtomcat7-java packages before 7.0.52-1ubuntu0.7 on Ubuntu 14.04 LTS, and tomcat8 and libtomcat8-java packages before 8.0.32-1ubuntu1.2 on Ubuntu 16.04 LTS allows local users with access to		A-APA-TOMCA--201016/78

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			the tomcat account to gain root privileges via a symlink attack on the Catalina log file, as demonstrated by /var/log/tomcat7/catalina.out. **Reference: CVE-2016-1240**		
Gain Privileges	2016-10-14	7.2	The Tomcat package on Red Hat Enterprise Linux (RHEL) 5 through 7, JBoss Web Server 3.0, and JBoss EWS 2 uses weak permissions for (1) /etc/sysconfig/tomcat and (2) /etc/tomcat/tomcat.conf, which allows local users to gain privileges by leveraging membership in the tomcat group. **Reference: CVE-2016-6325**	https://bugzilla.redhat.com/show_bug.cgi?id=1367447	A-APA-TOMCA--201016/79
Bb&t					
The U The U by BB&T mobile banking app for iPhone, iPad and Android.					
Gain Information	2016-10-05	4.3	The U by BB&T app 1.5.4 and earlier for iOS does not properly verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **Reference: CVE-2016-6550**	http://www.kb.cert.org/vuls/id/338624	A-BB&-THEU--201016/80
Beckhoff					
Embedded Pc Images; Twincat TwinCAT (The Windows Control and Automation Technology) automation suite forms the core of the control system. The TwinCAT software system turns almost any PC-based system into a real-time control with multiple PLC, NC, CNC and/or robotics runtime systems.					
NA	2016-10-05	9.4	Beckhoff Embedded PC	https://ics-	A-BEC-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			images before 2014-10-22 and Automation Device Specification (ADS) TwinCAT components might allow remote attackers to obtain access via the (1) Windows CE Remote Configuration Tool, (2) CE Remote Display service, or (3) TELNET service. **Reference: CVE-2014-5415**	cert.us-cert.gov/advisories/ICSA-16-278-02	EMBED--201016/81
Embedded Pc Images; Twincat TwinCAT (The Windows Control and Automation Technology) automation suite forms the core of the control system. The TwinCAT software system turns almost any PC-based system into a real-time control with multiple PLC, NC, CNC and/or robotics runtime systems.					
NA	2016-10-05	9.4	Beckhoff Embedded PC images before 2014-10-22 and Automation Device Specification (ADS) TwinCAT components do not restrict the number of authentication attempts, which makes it easier for remote attackers to obtain access via a brute-force attack. **Reference: CVE-2014-5414**	https://ics-cert.us-cert.gov/advisories/ICSA-16-278-02	A-BEC-EMBED--201016/82
Browserweb					
Whizz WHIZZ helps you quickly organize, manage and add a color-coded interface to your WordPress Admin.					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin whizz v1.0.7 **Reference: CVE-2016-1000154**		A-BRO-WHIZZ--201016/83
Candidate-application-form Project					
Candidate-application-form The Candidate Application Form is simple WordPress plugin which will create an application form which can be attached to a posted job vacancy, using a shortcode.					
Directory Traversal	2016-10-07	5	Remote file download vulnerability in candidate-application-form v1.0	http://www.vapidlabs.com/advisory.php?	A-CAN-CANDI--201016/84

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			wordpress plugin **Reference: CVE-2015-1000005**	v=142	
Ceph Project; Redhat					
Ceph/Ceph Storage Ceph is open source software designed to provide highly scalable object-, block- and file-based storage under a unified system. Ceph storage clusters are designed to run on commodity hardware, using an algorithm called CRUSH (Controlled Replication Under Scalable Hashing) to ensure data is evenly distributed across the cluster and that all cluster nodes can retrieve data quickly without any centralized bottlenecks.					
NA	2016-10-04	4.3	The RGW code in Ceph before 10.0.1, when authenticated-read ACL is applied to a bucket, allows remote attackers to list the bucket contents via a URL. **Reference: CVE-2016-7031**	https://github.com/ceph/ceph/pull/6057	A-CEP-CEPH/--201016/85
Cisco					
Adaptive Security Appliance Cisco Adaptive Security Appliance is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides proactive threat defense that stops attacks before they spread through the network.					
Denial of Service	2016-10-06	6.1	The DHCP Relay implementation in Cisco Adaptive Security Appliance (ASA) Software 8.4.7.29 and 9.1.7.4 allows remote attackers to cause a denial of service (interface wedge) via a crafted rate of DHCP packet transmission, aka Bug ID CSCuy66942. **Reference: CVE-2016-6424**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-asa-dhcp	A-CIS-ADAPT--201016/86
Content Security Management Appliance; Email Security Appliance; Web Security Appliance The Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email and web security appliances. It simplifies administration and planning, improves compliance monitoring, helps to enable consistent enforcement of policy, and enhances threat protection; The Email Security Appliance is the industry's first proven zero-hour antivirus solution. It offers a best-in-class capability to control and encrypt sensitive outbound email. At the same time, its layered defense, built into a single appliance, quickly blocks incoming attacks; Cisco Web Security Appliance simplifies security with a high-performance, dedicated appliance.					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service; Overflow	2016-10-05	4.3	The FTP service in Cisco AsyncOS on Email Security Appliance (ESA) devices 9.6.0-000 through 9.9.6-026, Web Security Appliance (WSA) devices 9.0.0-162 through 9.5.0-444, and Content Security Management Appliance (SMA) devices allows remote attackers to cause a denial of service via a flood of FTP traffic, aka Bug IDs CSCuz82907, CSCuz84330, and CSCuz86065. **Reference: CVE-2016-6416**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-aos	A-CIS-CONTE--201016/87
Firepower Management Center The Cisco Firepower Management Center is the administrative nerve center for a number of Ciscosecurity products running on a number of different platforms. It provides complete and unified management of firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.					
Execute Code	2016-10-05	6	SQL injection vulnerability in Cisco Firepower Management Center 4.10.3 through 5.4.0 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors, aka Bug ID CSCur25485. **Reference: CVE-2016-6419**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-fpmc	A-CIS-FIREP--201016/88
Gain Information	2016-10-06	4	The web console in Cisco Firepower Management Center 6.0.1 allows remote authenticated users to read arbitrary files via crafted parameters, aka Bug ID CSCva30376. **Reference: CVE-2016-6435**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ftmc2	A-CIS-FIREP--201016/89
Gain Information	2016-10-06	4.6	Cisco Firepower Management Center 6.0.1	http://tools.cisco.com/secur	A-CIS-FIREP--201016/90

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			has hardcoded database credentials, which allows local users to obtain sensitive information by leveraging CLI access, aka Bug ID CSCva30370. **Reference: CVE-2016-6434**	ity/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ftmc1	
Execute Code	2016-10-06	9	The Threat Management Console in Cisco Firepower Management Center 5.2.0 through 6.0.1 allows remote authenticated users to execute arbitrary commands via crafted web-application parameters, aka Bug ID CSCva30872. **Reference: CVE-2016-6433**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ftmc	A-CIS-FIREP--201016/91
Firesight System Software The Cisco FireSIGHT System combines the security of an industry-leading network intrusion protection system with the power to control access to your network based on detected applications, users, and URLs.					
Gain Privileges; Bypass	2016-10-05	6.8	Cisco FireSIGHT System Software 4.10.3 through 5.4.0 in Firepower Management Center allows remote authenticated users to bypass authorization checks and gain privileges via a crafted HTTP request, aka Bug ID CSCur25467. **Reference: CVE-2016-6420**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-fmc1	A-CIS-FIRES--201016/92
Cross Site Request Foregery	2016-10-05	6.8	Cross-site request forgery (CSRF) vulnerability in Cisco FireSIGHT System Software 4.10.2 through 6.1.0 and Firepower Management Center allows remote attackers to hijack the authentication of arbitrary users, aka Bug ID CSCva21636.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-fmc	A-CIS-FIRES--201016/93

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Reference: CVE-2016-6417		
Hostscan Engine NA					
Cross-site scripting	2016-10-06	4.3	Cross-site scripting (XSS) vulnerability in HostScan Engine 3.0.08062 through 3.1.14018 in the Cisco Host Scan package, as used in ASA Web VPN, allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCuz14682. **Reference: CVE-2016-6436**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-chs	A-CIS-HOSTS--201016/94
Nx-os NX-OS is a network operating system for the Nexus-series Ethernet switches and MDS-series Fibre Channel storage area network switches made by Cisco Systems.					
Execute Code; Overflow	2016-10-06	10	Buffer overflow in the Overlay Transport Virtualization (OTV) GRE feature in Cisco NX-OS 5.0 through 7.3 on Nexus 7000 and 7700 devices allows remote attackers to execute arbitrary code via long parameters in a packet header, aka Bug ID CSCuy95701. **Reference: CVE-2016-1453**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-otv	A-CIS-NX-OS--201016/95
Gain Information	2016-10-07	5	Cisco NX-OS before 7.0(3)I2(2e) and 7.0(3)I4 before 7.0(3)I4(1) has an incorrect iptables local-interface configuration, which allows remote attackers to obtain sensitive information via TCP or UDP traffic, aka Bug ID CSCuz05365. **Reference: CVE-2016-1455**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-n9kinfo	A-CIS-NX-OS--201016/96

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Unified Contact Center Express; Unified Intelligence Center Cisco Unified Contact Center Express offers Sophisticated call routing and comprehensive contact management capabilities. E-mail, Web Chat and social media integration; Unified Intelligence Center extend the boundaries of traditional contact center reporting. Unified Intelligence Center creates a comprehensive information portal where Contact Center reports and dashboards can be developed and shared throughout your organization.					
Cross Site Request Forgery	2016-10-06	6.8	Cross-site request forgery (CSRF) vulnerability in Cisco Unified Intelligence Center (CUIC) 8.5.4 through 9.1(1), as used in Unified Contact Center Express 10.0(1) through 11.0(1), allows remote attackers to hijack the authentication of arbitrary users, aka Bug IDs CSCuy75036 and CSCuy81654. **Reference: CVE-2016-6427**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis3	A-CIS-UNIFI--201016/97
NA	2016-10-06	4.3	The j_spring_security_switch_user function in Cisco Unified Intelligence Center (CUIC) 8.5.4 through 9.1(1), as used in Unified Contact Center Express 10.0(1) through 11.0(1), allows remote attackers to create user accounts by visiting an unspecified web page, aka Bug IDs CSCuy75027 and CSCuy81653. **Reference: CVE-2016-6426**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis2	A-CIS-UNIFI--201016/98
Cross-site scripting	2016-10-06	4.3	Cross-site scripting (XSS) vulnerability in Cisco Unified Intelligence Center (CUIC) 8.5.4 through 9.1(1), as used in Unified Contact Center Express 10.0(1) through 11.0(1), allows remote attackers to inject arbitrary web script or	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis1	A-CIS-UNIFI--201016/99

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			HTML via a crafted URL, aka Bug IDs CSCuy75020 and CSCuy81652. **Reference: CVE-2016-6425**		
Videoscape Distribution Suite Service Manager Cisco Videoscape Distribution Suite Service Manager (VDS-SM) is the reporting and analytics arm of the Videoscape Distribution Suite (VDS) products. It provides CDN Insights by ingesting logs from VDS IS product that represents the CDN delivery infrastructure.					
Cross-site scripting	2016-10-05	4.3	Cross-site scripting (XSS) vulnerability in Cisco Videoscape Distribution Suite Service Manager (VDS-SM) 3.0 through 3.4.0 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCva14552. **Reference: CVE-2016-6418**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-vds	A-CIS-VIDEO--201016/100
Citrix					
License Server;License Server Vpx Citrix License Server is a lightweight component that can be installed on the same system as a Citrix product for smaller deployments, or on one or more dedicated systems for larger deployments.					
Denial of Service	2016-10-11	5	The lmadmin component in Flexera FlexNet Publisher (aka Flex License Manager) before 2015 SP5 and 2016 before R1 SP1, as used by Citrix License Server for Windows before 11.14.0.1 and Citrix License Server VPX before 11.14.0.1, allow remote attackers to cause a denial of service (crash) via a type 2F packet with a '01 19' opcode. **Reference: CVE-2016-6273**	http://support.citrix.com/article/CTX217430	A-CIT-LICEN--201016/101
Contus-video-comments Project					
Contus-video-comments NA					
Directory	2016-10-07	9.4	Unauthenticated remote .jpg	http://www.v	A-CON-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Traversal			file upload in contus-video-comments v1.0 wordpress plugin **Reference: CVE-2016-1000112**	apidlabs.com/advisory.php?v=163	CONTU--201016/102
Defa-online-image-protector Project					
Defa-online-image-protector Defa Online Image Protector - Protect your image from download by browser and external software and also hotlinking.					
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin defa-online-image-protector v3.3 **Reference: CVE-2016-1000129**		A-DEF-DEFA--201016/103
Designsandcode					
Forget About Shortcode (FASC) Buttons are a visual way to add CSS buttons in the post editor screen and to your themes. Instead of adding shortcodes in the post editor, you insert real, styled buttons - making the process of adding buttons to your posts and pages much more natural whilst improving the appearance and usability of the post editor.					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin forget-about-shortcode-buttons v1.1.1 **Reference: CVE-2016-1000133**		A-DES-FORGE--201016/104
Drupal					
DukaPress is open source software that can be used to build online shops quickly and easily. DukaPress is built on top of WordPress, a world class content management system. DukaPress is built to be both simple and elegant yet powerful and scalable.					
Bypass	2016-10-04	4	The system.temporary route in Drupal 8.x before 8.1.10 does not properly check for "Export configuration" permission, which allows remote authenticated users to bypass intended access restrictions and read a full config export via unspecified vectors. **Reference: CVE-2016-7572**	https://www.drupal.org/SA-CORE-2016-004	A-DRU-DRUPA--201016/105
Cross-site scripting	2016-10-04	4.3	Cross-site scripting (XSS) vulnerability in Drupal 8.x before 8.1.10 allows remote	https://www.drupal.org/SA-CORE-2016-	A-DRU-DRUPA--201016/106

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			attackers to inject arbitrary web script or HTML via vectors involving an HTTP exception. **Reference: CVE-2016-7571**	004	
NA	2016-10-04	4	Drupal 8.x before 8.1.10 does not properly check for "Administer comments" permission, which allows remote authenticated users to set the visibility of comments for arbitrary nodes by leveraging rights to edit those nodes. **Reference: CVE-2016-7570**	https://www.drupal.org/SA-CORE-2016-004	A-DRU-DRUPA--201016/107
Dukapress Project					
Dukapress DukaPress is open source software that can be used to build online shops quickly and easily. DukaPress is built on top of WordPress, a world class content management system. DukaPress is built to be both simple and elegant yet powerful and scalable.					
SQL Injection	2016-10-07	7.5	Blind SQL Injection in wordpress plugin dukapress v2.5.9 **Reference: CVE-2015-1000011**		A-DUK-DUKAP--201016/108
EMC					
Networker Module For Microsoft Applications;Replication Manager To simplify protection and recovery of Microsoft environments, EMC NetWorker and the NetWorker Module for Microsoft provide a single, unified solution that leverages Microsoft Volume Shadow Copy Service (VSS) for snapshot-based protection and recovery of Microsoft Exchange, SQL, SharePoint, and Active Directory, as well as SQL VDI for transaction log-based backup;Automate the entire data replication process through a centralized management console with EMC Replication Manager replication software.					
Execute Code	2016-10-05	7.5	The client in EMC Replication Manager (RM) before 5.5.3.0_01-PatchHotfix, EMC Network Module for Microsoft 3.x, and EMC Networker Module for Microsoft 8.2.x before 8.2.3.6 allows remote RM	http://seclists.org/bugtraq/2016/Oct/6	A-EMC-NETWO--201016/109

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			servers to execute arbitrary commands by placing a crafted script in an SMB share. **Reference: CVE-2016-0913**		
Solutions Enabler;Unisphere The EMC Solutions Enabler software provides your host system with an API shared library and a special command set that comprises the Symmetrix Command Line Interface (SYMCLI);Unisphere provides a flexible, integrated experience for managing existing EMC CLARiiON and EMC Celerra storage systems as well as next-generation EMC unified storage the EMC VNX and EMC VNXe series.					
Execute Code	2016-10-06	10	The vApp Managers web application in EMC Unisphere for VMAX Virtual Appliance 8.x before 8.3.0 and Solutions Enabler Virtual Appliance 8.x before 8.3.0 allows remote attackers to execute arbitrary code via crafted input to the (1) GetSymmCmdRequest or (2) RemoteServiceHandler class. **Reference: CVE-2016-6646**	http://seclists.org/bugtraq/2016/Oct/7	A-EMC-SOLUT--201016/110
Execute Code	2016-10-06	9	The vApp Managers web application in EMC Unisphere for VMAX Virtual Appliance 8.x before 8.3.0 and Solutions Enabler Virtual Appliance 8.x before 8.3.0 allows remote authenticated users to execute arbitrary code via crafted input to the (1) GeneralCmdRequest, (2) PersistantDataRequest, or (3) GetCommandExecRequest class. **Reference: CVE-2016-6645**	http://seclists.org/bugtraq/2016/Oct/7	A-EMC-SOLUT--201016/111

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

F5					
Big-ip Access Policy Manager;Big-ip Advanced Firewall Manager;Big-ip Application Acceleration Manager;Big-ip Application Security Manager;Big-ip Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Websafe BIG-IP Access Policy Manager is a flexible, high-performance access and security solution that provides unified global access to your applications, network, and cloud;BIG-IP Advanced Firewall Manager is a high-performance, stateful, full-proxy network security solution designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols;BIG-IP Application Acceleration Manager overcomes network, protocol, and application issues to help you meet application performance, data replication, and disaster recovery requirements presented by cloud, mobile applications, and video distribution;BIG-IP Application Security Manager is a flexible web application firewall that secures web applications in traditional, virtual, and private cloud environments;Big-ip Link Controller puts the management of these links under your control.					
Execute Code	2016-10-04	9.3	Virtual servers in F5 BIG-IP systems 11.5.0, 11.5.1 before HF11, 11.5.2, 11.5.3, 11.5.4 before HF2, 11.6.0 before HF8, 11.6.1 before HF1, 12.0.0 before HF4, and 12.1.0 before HF2, when configured with the HTTP Explicit Proxy functionality or SOCKS profile, allow remote attackers to modify the system configuration, read system files, and possibly execute arbitrary code via unspecified vectors. **Reference: CVE-2016-5700**	https://support.f5.com/kb/en-us/solutions/public/k/35/sol35520031.html	A-F5-BIG-I--201016/112
Big-ip Local Traffic Manager Big-ip Local Traffic Manager is it's a Full Proxy, allowing you to augment client and server side connections. All while making informed load balancing decisions on availability, performance, and persistence.					
NA	2016-10-05	10	F5 BIG-IP LTM systems 11.x before 11.2.1 HF16, 11.3.x, 11.4.x before 11.4.1 HF11, 11.5.0, 11.5.1 before HF11, 11.5.2, 11.5.3, 11.5.4 before HF2, 11.6.0 before HF8, 11.6.1 before HF1, 12.0.0 before HF4, and 12.1.0 before HF2 allow remote attackers to modify or extract system configuration	https://support.f5.com/kb/en-us/solutions/public/k/64/sol64743453.html	A-F5-BIG-I--201016/113

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			files via vectors involving NAT64. **Reference: CVE-2016-5745**		
Fast-image-adder Project					
Fast-image-adder NA					
NA	2016-10-07	5	Remote file upload vulnerability in fast-image-adder v1.1 Wordpress plugin **Reference: CVE-2015-1000001**	NA	A-FAS-FAST---201016/114
Filedownload Project					
Filedownload File Download is a cross server platform compatible jQuery plugin that allows for an Ajax-like file download experience that isn't normally possible using the web.					
Cross-site scripting	2016-10-11	4.3	Open Proxy in filedownload v1.4 wordpress plugin **Reference: CVE-2015-1000004**	NA	A-FIL-FILED--201016/115
SQL Injection	2016-10-11	7.5	Open Proxy in filedownload v1.4 wordpress plugin **Reference: CVE-2015-1000003**	NA	A-FIL-FILED--201016/116
NA	2016-10-11	5.8	Open Proxy in filedownload v1.4 wordpress plugin **Reference: CVE-2015-1000002**	NA	A-FIL-FILED--201016/117
Flask-oidc Project					
Flask-oidc Flask-OIDC is an extension to Flask that allows you to add OpenID Connect based authentication to your website in a matter of minutes.					
NA	2016-10-12	5.8	flask-oidc version 0.1.2 and earlier is vulnerable to an open redirect **Reference: CVE-2016-1000001**	NA	A-FLA-FLASK--201016/118
Fortinet					
Fortiwlc The FortiWLC controller series optimizes traffic across infrastructure wireless access points and client devices to support high density, high performance and predictability while addressing mission-critical enterprise demands for wireless connectivity.					
Gain Information	2016-10-05	4	Fortinet FortiWLC 6.1-2-29 and earlier, 7.0-9-1, 7.0-10-0, 8.0-5-0, 8.1-2-0, and 8.2-4-0	http://fortiguard.com/advisory/F	A-FOR-FORTI--201016/119

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			allow administrators to obtain sensitive user credentials by reading the pam.log file. **Reference: CVE-2016-7561**	G-IR-16-030	
NA	2016-10-05	10	The rsyncd server in Fortinet FortiWLC 6.1-2-29 and earlier, 7.0-9-1, 7.0-10-0, 8.0-5-0, 8.1-2-0, and 8.2-4-0 has a hardcoded rsync account, which allows remote attackers to read or write to arbitrary files via unspecified vectors. **Reference: CVE-2016-7560**	http://fortiguard.com/advisory/FG-IR-16-029	A-FOR-FORTI--201016/120
Freerdp Project					
Freerdp FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license.					
Denial of Service	2016-10-04	5	FreeRDP before 1.1.0-beta+2013071101 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) by disconnecting before authentication has finished. **Reference: CVE-2013-4119**	https://github.com/FreeRDP/FreeRDP/commit/0773bb9303d24473fe1185d85a424dfe159aff53	A-FRE-FREER--201016/121
Google-adsense-and-hotel-booking Project					
Google-adsense-and-hotel-booking NA					
NA	2016-10-13	6.4	Open proxy in Wordpress plugin google-adsense-and-hotel-booking v1.05 **Reference: CVE-2015-1000009**	NA	A-GOO-GOOGL--201016/122
Hdw-tube Project					
Hdw-tube NA					
Cross-site scripting	2016-10-12	4.3	Reflected Cross-site scripting in wordpress plugin hdw-tube v1.2 **Reference: CVE-2016-1000135**	NA	A-HDW-HDW-T--201016/123
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin hdw-tube v1.2 **Reference: CVE-2016-**	NA	A-HDW-HDW-T--201016/124

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			1000134		
Heat-trakr Project					
Heat-trackr Heat trackr plugin allows the user to display heatmaps, clickmaps, scattermaps and scrollmaps plus perform A/B split testing.					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin heat-trackr v1.0 **Reference: CVE-2016-1000136**	NA	A-HEA-HEAT--201016/125
Hero-maps-pro Project					
Hero-maps-pro The Hero Maps plugin allows for quick and easy Google Maps addition to your WordPress website.					
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin hero-maps-pro v2.1.0 **Reference: CVE-2016-1000137**	NA	A-HER-HERO--201016/126
HP					
Keyview HP KeyView file filtering and transformation software enables you to extract content and metadata from virtually all file formats.					
Execute Code	2016-10-05	6.8	The Filter SDK in HPE KeyView 10.18 through 10.24 allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4387, CVE-2016-4388, and CVE-2016-4389. **Reference: CVE-2016-4390**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05297477	A-HP-KEYVI--201016/127
Execute Code	2016-10-05	6.8	The Filter SDK in HPE KeyView 10.18 through 10.24 allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4387, CVE-2016-4388, and CVE-2016-4390. **Reference: CVE-2016-4389**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05297477	A-HP-KEYVI--201016/128
Execute Code	2016-10-05	6.8	The Filter SDK in HPE KeyView 10.18 through 10.24 allows remote attackers to execute arbitrary code via unspecified vectors, a different	https://h20566.www2.hpe.com/portal/site/hpsc/public/k	A-HP-KEYVI--201016/129

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			vulnerability than CVE-2016-4387, CVE-2016-4389, and CVE-2016-4390. **Reference: CVE-2016-4388**	b/docDisplay?docId=emr_na-c05297477	
Execute Code	2016-10-05	6.8	The Filter SDK in HPE KeyView 10.18 through 10.24 allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4388, CVE-2016-4389, and CVE-2016-4390. **Reference: CVE-2016-4387**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05297477	A-HP-KEYVI--201016/130
Huawei					
Esight Huawei eSight ICT Infrastructure Management System simplifies and automates network management of converged data center and enterprise networks.					
Directory Traversal	2016-10-04	4	Directory traversal vulnerability in Huawei eSight before V300R003C20SPC005 allows remote authenticated users to read arbitrary files via unspecified vectors. **Reference: CVE-2016-8280**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160928-01-pathtraversal-en	A-HUA-ESIGH--201016/131
Usg2100;Usg2200;Usg5100;Usg5500 The USG5500 series is a new 10-Gigabit unified security gateway, developed by Huawei to meet the needs of carriers, large and medium sized enterprises, and next-generation data centers. The USG5500 series integrates large-capacity switching with dedicated security defense capabilities, including IPS, anti-virus (AV), URL filtering, application control, and anti-spam (AS) technologies.					
Denial of Service; Execute Code; Overflow	2016-10-04	9.3	Buffer overflow in the Point-to-Point Protocol over Ethernet (PPPoE) module in Huawei USG2100, USG2200, USG5100, and USG5500 unified security gateways with software before V300R001C10SPC600, when CHAP authentication is configured on the server, allows remote attackers to	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160914-01-usg-en	A-HUA-USG21--201016/132

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			cause a denial of service (server restart) or execute arbitrary code via crafted packets sent during authentication. **Reference: CVE-2016-8276**		
Usg9520;Usg9560;Usg9580 By using dedicated multi-core chips and a distributed hardware platform, the USG9520, USG9560 provides industry leading service processing and expansion capabilities; Huawei USG9580 firewall security platform has successfully completed independent third-party testing and evaluation by NSS Labs. Huawei's USG9500 series passed various tests and satisfied all requirements contained within the NSS Labs "Firewall Testing Methodology".					
Denial of Service	2016-10-06	7.8	Huawei USG9520, USG9560, and USG9580 unified security gateways with software before V300R001C01SPCa00 allow remote attackers to cause a denial of service (device restart) via an unspecified URL. **Reference: CVE-2016-8278**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160921-02-firewall-en	A-HUA-USG95--201016/133
Denial of Service	2016-10-06	6.8	Huawei USG9520, USG9560, and USG9580 unified security gateways with software before V300R001C01SPCa00 allow remote authenticated users to cause a denial of service (device restart) via an unspecified command parameter. **Reference: CVE-2016-8277**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160921-01-firewall-en	A-HUA-USG95--201016/134
Huge-it					
Huge-it Catalog Huge-IT Product Catalog is made for demonstration, sale, advertisements for your products. Imagine a stand with a variety of catalogs with a specific product.					
SQL Injection	2016-10-07	7.5	Unauthenticated SQL Injection in Huge-IT Catalog v1.0.7 for Joomla **Reference: CVE-2016-1000125**	NA	A-HUG-HUGE--201016/135
Huge-it Image Gallery Huge-IT Image Gallery plugin is a modern way to demonstrate your images as well as videos. Plugin includes 7 nicely designed views; using them you can make your website look more lively and pleasant					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

for your visitors.					
Cross-site scripting	2016-10-07	4.3	XSS in huge IT gallery v1.1.5 for Joomla **Reference: CVE-2016-1000114**	NA	A-HUG-HUGE---201016/136
SQL Injection; Cross-site scripting	2016-10-07	7.5	XSS and SQLi in huge IT gallery v1.1.5 for Joomla **Reference: CVE-2016-1000113**	NA	A-HUG-HUGE---201016/137
Portfolio Gallery Portfolio is perfect for using for creating various portfolios within various views. The product allows adding unlimited projects containing images, videos, descriptions and titles for each portfolio. It is rather useful weather using with various pages and posts, as well as within custom location.					
SQL Injection	2016-10-07	7.5	Unauthenticated SQL Injection in Huge-IT Portfolio Gallery Plugin v1.0.6 **Reference: CVE-2016-1000124**	NA	A-HUG-PORTF--201016/138
Video Gallery Video Gallery plugin was created and specifically designed to show your videos from Vimeo and Youtube in unusual splendid ways.					
SQL Injection	2016-10-07	7.5	Unauthenticated SQL Injection in Huge-IT Video Gallery v1.0.9 for Joomla **Reference: CVE-2016-1000123**	NA	A-HUG-VIDEO--201016/139
IBM					
B2b Advanced Communications; Multi-enterprise Integration Gateway B2B Advanced Communications provides optimized and dynamic end-to-end information flows in optimized and dynamic end-to-end information.					
Cross-site scripting	2016-10-05	3.5	Cross-site scripting (XSS) vulnerability in IBM 10x, as used in Multi-Enterprise Integration Gateway 1.x through 1.0.0.1 and B2B Advanced Communications before 1.0.0.5_2, allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5892**	http://www-01.ibm.com/support/docview.wss?uid=swg21991148	A-IBM-B2B A--201016/140
Business Process Manager Business process management (BPM) is a field in operations management that focuses on improving					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

corporate performance by managing and optimizing a company's business processes.					
Cross-site scripting	2016-10-05	3.5	Cross-site scripting (XSS) vulnerability in a test page in IBM Business Process Manager Advanced 8.5.6.0 through 8.5.7.0 before cumulative fix 2016.09 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5901**	http://www-01.ibm.com/support/docview.wss?uid=swg21990852	A-IBM-BUSIN--201016/141
Sterling Secure Proxy IBM Sterling Secure Proxy provides a demilitarized zone (DMZ)-based application proxy that shields file transfers from the public Internet.					
Cross-site scripting; Gain Information	2016-10-07	5.8	The Configuration Manager in IBM Sterling Secure Proxy (SSP) 3.4.2 before 3.4.2.0 iFix 8 and 3.4.3 before 3.4.3.0 iFix 1 does not enable the HSTS protection mechanism, which makes it easier for remote attackers to obtain sensitive information or modify data by leveraging use of HTTP. **Reference: CVE-2016-6027**	http://www-01.ibm.com/support/docview.wss?uid=swg21991278	A-IBM-STERL--201016/142
Gain Information	2016-10-07	2.9	The Configuration Manager in IBM Sterling Secure Proxy (SSP) 3.4.2 before 3.4.2.0 iFix 8 and 3.4.3 before 3.4.3.0 iFix 1 allows man-in-the-middle attackers to obtain sensitive information via an HTTP method that is neither GET nor POST. **Reference: CVE-2016-6026**	http://www-01.ibm.com/support/docview.wss?uid=swg21991278	A-IBM-STERL--201016/143
NA	2016-10-07	4.6	The Configuration Manager in IBM Sterling Secure Proxy (SSP) 3.4.2 before 3.4.2.0 iFix 8 and 3.4.3 before 3.4.3.0 iFix 1 allows remote attackers to obtain access by leveraging an unattended workstation to conduct a post-logoff session-	http://www-01.ibm.com/support/docview.wss?uid=swg21991278	A-IBM-STERL--201016/144

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			reuse attack involving a modified URL. **Reference: CVE-2016-6025**		
Directory Traversal	2016-10-07	5	Directory traversal vulnerability in the Configuration Manager in IBM Sterling Secure Proxy (SSP) 3.4.2 before 3.4.2.0 iFix 8 and 3.4.3 before 3.4.3.0 iFix 1 allows remote attackers to read arbitrary files via a crafted URL. **Reference: CVE-2016-6023**	http://www-01.ibm.com/support/docview.wss?uid=swg21991278	A-IBM-STERL--201016/145
Websphere Application Server WebSphere Application Server (WAS) is a software framework and middleware that hosts Java based web applications. It is the flagship product within IBM's WebSphere software suite.					
Execute Code	2016-10-05	6.5	IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.43, 8.0 before 8.0.0.13, 8.5 before 8.5.5.11, 9.0 before 9.0.0.2, and Liberty before 16.0.0.4 allows remote authenticated users to execute arbitrary Java code via a crafted serialized object. **Reference: CVE-2016-5983**	https://www-01.ibm.com/support/docview.wss?uid=swg21990060	A-IBM-WEBSP--201016/146
Indasengineering					
Web Scada A pure web SCADA can display all mimic animation and control, trending, alarm, report and so on directly and securely in any modern browsers.					
Directory Traversal	2016-10-05	5	Directory traversal vulnerability in INDAS Web SCADA before 3 allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2016-8343**	https://ics-cert.us-cert.gov/advisories/ICSA-16-278-01	A-IND-WEB S--201016/147
Indexisto Project					
Indexisto: NA					
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin indexisto v1.0.5 **Reference: CVE-2016-1000138**	NA	A-IND-INDEX--201016/148

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Infusionsoft Project					
Infusionsoft Sales and marketing automation software built exclusively for small business success.					
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin infusionsoft v1.5.11 **Reference: CVE-2016-1000139**	NA	A-INF-INFUS--201016/149
Intel					
Integrated Performance Primitives Intel Integrated Performance Primitives (Intel IPP) is a multi-threaded software library of functions for multimedia and data processing applications, produced by Intel.					
Gain Information	2016-10-12	2.1	Intel Integrated Performance Primitives (aka IPP) Cryptography before 9.0.4 makes it easier for local users to discover RSA private keys via a side-channel attack. **Reference: CVE-2016-8100**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00060&languageid=en-fr	A-INT-INTEG--201016/150
Solid-state Drive Toolbox The Intel Solid-State Drive Toolbox is drive management software that allows you to view current drive information for Solid-State Drives, such as Drive Health, Estimated Life Remaining, SMART attributes, Drive Details, Optimize the performance of an Intel SSD and Check and tune your system settings.					
Gain Privileges	2016-10-12	7.2	The updater subsystem in Intel SSD Toolbox before 3.3.7 allows local users to gain privileges via unspecified vectors. **Reference: CVE-2016-8101**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00061&languageid=en-fr	A-INT-SOLID--201016/151
Ipswitch					
Whatsup Gold WhatsUp Gold is a unified application, server and network monitoring software solution featuring the industry's most flexible licensing model.					
SQL Injection	2016-10-07	6.5	Ipswitch WhatsUp Gold 16.4.1 WrFreeFormText.asp sUniqueID Parameter Blind SQL Injection	http://www.tenable.com/security/research/	A-IPS-WHATS--201016/152

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Reference: CVE-2016-1000000	tra-2016-15	
Libtiff					
Libtiff Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files. The set also contains command line tools for processing TIFFs.					
Denial of Service	2016-10-03	5	The cvtClump function in the rgb2ycbcr tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) by setting the "-v" option to -1. **Reference: CVE-2016-3624**	NA	A-LIB-LIBTI--201016/153
Denial of Service	2016-10-03	4.3	The fpAcc function in tif_predict.c in the tiff2rgba tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted TIFF image. **Reference: CVE-2016-3622**	http://www.openwall.com/lists/oss-security/2016/04/07/4	A-LIB-LIBTI--201016/154
Denial of Service	2016-10-03	6.8	The LZWEncode function in tif_lzw.c in the bmp2tiff tool in LibTIFF 4.0.6 and earlier, when the "-c lzw" option is used, allows remote attackers to cause a denial of service (buffer over-read) via a crafted BMP image. **Reference: CVE-2016-3621**	NA	A-LIB-LIBTI--201016/155
Denial of Service	2016-10-03	5	The ZIPEncode function in tif_zip.c in the bmp2tiff tool in LibTIFF 4.0.6 and earlier, when the "-c zip" option is used, allows remote attackers to cause a denial of service (buffer over-read) via a crafted BMP image. **Reference: CVE-2016-3620**	NA	A-LIB-LIBTI--201016/156
Denial of Service	2016-10-03	4.3	The DumpModeEncode function in tif_dumpmode.c in the bmp2tiff tool in LibTIFF 4.0.6 and earlier, when the "-c	NA	A-LIB-LIBTI--201016/157

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			none" option is used, allows remote attackers to cause a denial of service (buffer over-read) via a crafted BMP image. **Reference: CVE-2016-3619**		
Libtiff Project					
Libtiff Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files. The set also contains command line tools for processing TIFFs.					
Denial of Service	2016-10-03	5	The TIFFWriteDirectoryTagLongLong8Array function in tif_dirwrite.c in the tiffset tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving the ma variable. **Reference: CVE-2016-3658**	NA	A-LIB-LIBTI--201016/158
Denial of Service	2016-10-03	5	The tagCompare function in tif_dirinfo.c in the thumbnail tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to field_tag matching. **Reference: CVE-2016-3634**	NA	A-LIB-LIBTI--201016/159
Denial of Service	2016-10-03	5	The setrow function in the thumbnail tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the src variable. **Reference: CVE-2016-3633**	NA	A-LIB-LIBTI--201016/160
Denial of Service	2016-10-03	4.3	tif_read.c in the tiff2bw tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TIFF image. **Reference: CVE-2016-3625**	NA	A-LIB-LIBTI--201016/161

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service	2016-10-06	5	The (1) cpStrips and (2) cpTiles functions in the thumbnail tool in LibTIFF 4.0.6 and earlier allow remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the bytecounts[] array variable. **Reference: CVE-2016-3631**	http://www.openwall.com/lists/oss-security/2016/04/08/10	A-LIB-LIBTI--201016/162
Mailcwp Project					
Mailcwp MailCWP is designed to be responsive and feature rich. Powered by jQuery and AJAX the system responds quickly to user requests.					
NA	2016-10-07	5	Remote file upload vulnerability in mailcwp v1.99 wordpress plugin **Reference: CVE-2015-1000000**	NA	A-MAI-MAILC--201016/163
Microsoft					
Edge Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems.					
Execute Code; Overflow	2016-10-14	9.3	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Remote Code Execution Vulnerability." **Reference: CVE-2016-7189**	http://technet.microsoft.com/en-us/security/bulletin/ms16-119	A-MIC-EDGE--201016/164
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	9.3	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3389, CVE-2016-7190, and CVE-2016-7194. **Reference: CVE-2016-3386**	http://technet.microsoft.com/en-us/security/bulletin/ms16-119	A-MIC-EDGE--201016/165

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Microsoft					
Edge; Internet Explorer Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems, replacing Internet Explorer as the default web browser on all device classes.					
Gain Privileges	2016-10-14	9.3	Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private namespaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Browser Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3387. **Reference: CVE-2016-3388**	NA	A-MIC-EDGE;--201016/166
Gain Privileges	2016-10-14	6.8	Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private namespaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Browser Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3388. **Reference: CVE-2016-3387**	NA	A-MIC-EDGE;--201016/167
Denial of Service;Execute Code Overflow;Memory Corruption	2016-10-14	9.3	The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as demonstrated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerability." **Reference: CVE-2016-3382**	NA	A-MIC-EDGE;--201016/168
Denial of Service;Execute	2016-10-14	9.3	Microsoft Internet Explorer 11 and Microsoft Edge allow	NA	A-MIC-EDGE;--201016/169

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Code Overflow;Memory Corruption			remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference: CVE-2016-3331**		
Gain Information	2016-10-14	4.3	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to determine the existence of unspecified files via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." **Reference: CVE-2016-3267**	NA	A-MIC-EDGE;--201016/170
Internet Explorer Internet Explorer graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995.					
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	9.3	The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." **Reference: CVE-2016-3385**	http://technet.microsoft.com/en-us/security/bulletin/ms16-118	A-MIC-INTER--201016/171
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	9.3	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." **Reference: CVE-2016-3384**	http://technet.microsoft.com/en-us/security/bulletin/ms16-118	A-MIC-INTER--201016/172
Denial of Service; Execute Code Overflow; Memory Corruption	2016-10-14	9.3	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption)	http://technet.microsoft.com/en-us/security/bulletin/m	A-MIC-INTER--201016/173

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference: CVE-2016-3383**	s16-118	
Mirror Manager Project					
Mirror Manager MirrorManager keeps track of the nearly 400 public mirrors, and over 300 private mirrors, that carry Fedora, EPEL, and RHEL content, and is used by rpmfusion.org, a third-party repository.					
Execute Code	2016-10-11	7.5	Mirror Manager version 0.7.2 and older is vulnerable to remote code execution in the checkin code **Reference: CVE-2016-1000003**	NA	A-MIR-MIRRO--201016/174
Mp3-jplayer Project					
Mp3-jplayer Mp3-jplayer Flexible multi-player audio plugin. Near-continuous playback between pages.					
Gain Information	2016-10-11	5	Path Disclosure Vulnerability in wordpress plugin MP3-jPlayer v2.3.2 **Reference: CVE-2015-1000008**	NA	A-MP3-MP3-J--201016/175
Mypixs Project					
Mypixs: NA					
Gain Information ; File Inclusion	2016-10-07	5	Local File Inclusion Vulnerability in mypixs v0.3 wordpress plugin **Reference: CVE-2015-1000012**	NA	A-MYP-MYPIX--201016/176
New-year-firework Project					
New-year-firework: NA					
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin new-year-firework v1.1.9 **Reference: CVE-2016-1000140**	NA	A-NEW-NEW-Y--201016/177
Openstack					
Cinder; Glance; Nova OpenStack Block Storage (Cinder) provides persistent block-level storage devices for use with OpenStack compute instances; OpenStack Image (Glance) provides discovery, registration, and delivery services for disk and server images; OpenStack Compute (Nova) is a cloud computing fabric controller, which is the main part of an IaaS system.					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service	2016-10-11	7.8	The image parser in OpenStack Cinder 7.0.2 and 8.0.0 through 8.1.1; Glance before 11.0.1 and 12.0.0; and Nova before 12.0.4 and 13.0.0 does not properly limit qemu-img calls, which might allow attackers to cause a denial of service (memory and disk consumption) via a crafted disk image. **Reference: CVE-2015-5162**	https://launchpad.net/bugs/1449062	A-OPE-CINDE--201016/178
Oxil					
Simplified-content Simplified Content is a plugin hosted at WordPress.org which provides managers with a simple tool to target legacy browsers and automatically generate simplified content for those browsers.					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin simplified-content v1.0.0 **Reference: CVE-2016-1000150**	NA	A-OXI-SIMPL--201016/179
Page-layout-builder Project					
Page-layout-builder NA					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin page-layout-builder v1.9.3 **Reference: CVE-2016-1000141**	NA	A-PAG-PAGE--201016/180
Pagure Project					
Pagure Pagure is a git-centered forge, python based using pygit2.					
Cross-site scripting	2016-10-12	4.3	Pagure 2.2.1 XSS in raw file endpoint **Reference: CVE-2016-1000007**	NA	A-PAG-PAGUR--201016/181
Parsi-font Project					
Parsi-font: NA					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin parsi-font v4.2.5 **Reference: CVE-2016-1000142**	NA	A-PAR-PARSI--201016/182
Photoxhibit Project					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Photoxhibit: NA					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin photoxhibit v2.1.8 **Reference: CVE-2016-1000143**	NA	A-PHO-PHOTO--201016/183
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin photoxhibit v2.1.8 **Reference: CVE-2016-1000144**	NA	A-PHO-PHOTO--201016/184
Pivotal Software					
Cloud Foundry Cf Mysql Pivotal Services includes a highly available MySQL database. Applications running on Pivotal Cloud Foundry can now be backed by a resilient relational database.This integrated Database as a Service (DBaaS) ensures continuous availability of critical applications, without requiring the operational overhead of creating and managing a MySQL cluster.					
Gain Information	2016-10-06	5	The MariaDB audit_plugin component in Pivotal Cloud Foundry (PCF) cf-mysql-release 27 and 28 allows remote attackers to obtain sensitive information by reading syslog messages, as demonstrated by cleartext credentials. **Reference: CVE-2016-6653**	https://pivotal.io/security/cve-2016-6653	A-PIV-CLOUD--201016/185
Spring Data Jpa Spring Data JPA aims to significantly improve the implementation of data access layers by reducing the effort to the amount that's actually needed.					
Execute Code; SQL Injection	2016-10-06	6.8	SQL injection vulnerability in Pivotal Spring Data JPA before 1.9.6 (Gosling SR6) and 1.10.x before 1.10.4 (Hopper SR4), when used with a repository that defines a String query using the @Query annotation, allows attackers to execute arbitrary JPQL commands via a sort instance with a function call. **Reference: CVE-2016-6652**	https://jira.spring.io/browse/DATAJPA-965	A-PIV-SPRIN--201016/186
Pondol-carousel Project					
Pondol-carousel NA					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin pondol-carousel v1.0 **Reference: CVE-2016-1000145**	NA	A-PON-PONDO--201016/187
Pondol-formmail Project					
Pondol-formmail: NA					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin pondol-formmail v1.1 **Reference: CVE-2016-1000146**	NA	A-PON-PONDO--201016/188
Qemu					
Qemu QEMU supports virtualization when executing under the Xen hypervisor or using the KVM kernel module in Linux.					
Denial of Service	2016-10-05	4.9	The pcnet_rdra_addr function in hw/net/pcnet.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by setting the (1) receive or (2) transmit descriptor ring length to 0. **Reference: CVE-2016-7909**	NA	A-QEM-QEMU--201016/189
Denial of Service	2016-10-05	2.1	The mcf_fec_do_tx function in hw/net/mcf_fec.c in QEMU (aka Quick Emulator) does not properly limit the buffer descriptor count when transmitting packets, which allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via vectors involving a buffer descriptor with a length of 0 and crafted values in bd.flags. **Reference: CVE-2016-7908**	http://git.qemu.org/?p=qemu.git;a=commit;h=070c4b92b8cd5390889716677a0b92444d6e087a	A-QEM-QEMU--201016/190
Denial of Service	2016-10-05	2.1	The imx_fec_do_tx function in hw/net/imx_fec.c in QEMU (aka Quick Emulator) does not properly limit the buffer descriptor count when	NA	A-QEM-QEMU--201016/191

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			transmitting packets, which allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via vectors involving a buffer descriptor with a length of 0 and crafted values in bd.flags. **Reference: CVE-2016-7907**		
Execute Code;Overflow	2016-10-05	10	Heap-based buffer overflow in the .receive callback of xlnx.xps-ethernetlite in QEMU (aka Quick Emulator) allows attackers to execute arbitrary code on the QEMU host via a large ethlite packet. **Reference: CVE-2016-7161**	http://git.qemu.org/?p=qemu.git;a=commit;h=a0d1cbdacff5df4ded16b753b38fdd9da6092968	A-QEM-QEMU--201016/192
Denial of Service	2016-10-12	2.1	The mptsas_process_scsi_io_request function in QEMU (aka Quick Emulator), when built with LSI SAS1068 Host Bus emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors involving MPTSASRequest objects. **Reference: CVE-2016-7423**	http://git.qemu.org/?p=qemu.git;a=commit;h=670e56d3ed2918b3861d9216f2c0540d9e9ae0d5	A-QEM-QEMU--201016/193
Recent-backups Project					
Recent-backups: NA					
Directory Traversal	2016-10-07	5	Remote file download vulnerability in recent-backups v0.7 wordpress plugin **Reference: CVE-2015-1000006**	http://www.vapidlabs.com/advisory.php?v=144	A-REC-RECEN--201016/194
Redhat					
Cloudforms Management Engine Cloudforms gives flexibility while providing a unified and consistent set of management capabilities across Virtualization platforms like Red Hat Virtualization, VMware vRealize, and Microsoft Hyper-V.					
Execute Code	2016-10-11	9	Red Hat CloudForms	http://rhn.	A-RED-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Management Engine 4.1 does not properly handle regular expressions passed to the expression engine via the JSON API and the web-based UI, which allows remote authenticated users to execute arbitrary shell commands by leveraging the ability to view and filter collections. **Reference: CVE-2016-7040**	redhat.com /errata/RHSA-2016-1996.html	CLOUD--201016/195
Enterprise Virtualization Red Hat Enterprise Virtualization (RHEV), an enterprise virtualization product produced by Red Hat, based on the KVM hypervisor.					
Gain Information	2016-10-04	2.1	The ovirt-engine-provisiondb utility in Red Hat Enterprise Virtualization (RHEV) Engine 4.0 allows local users to obtain sensitive database provisioning information by reading log files. **Reference: CVE-2016-5432**	https://bugzilla.redhat.com/show_bug.cgi?id=1371428	A-RED-ENTER--201016/196
Jboss Bpm Suite Jboss Bpm Suite enables enterprise business and IT users to document, simulate, manage, automate and monitor business processes and policies.					
Cross-site scripting	2016-10-04	3.5	Cross-site scripting (XSS) vulnerability in Business Process Editor in Red Hat JBoss BPM Suite before 6.3.3 allows remote authenticated users to inject arbitrary web script or HTML by levering permission to create business processes. **Reference: CVE-2016-5398**	https://bugzilla.redhat.com/show_bug.cgi?id=1358523	A-RED-JBOSS--201016/197
Jboss Enterprise Application Platform The JBoss Enterprise Application Platform (or JBoss EAP) is a subscription-based/open-source Java EE-based application server runtime platform used for building, deploying, and hosting highly-transactional Java applications and services.					
Denial of Service	2016-10-04	7.1	Red Hat JBoss Enterprise Application Platform (EAP) 7, when operating as a reverse-proxy with default buffer sizes, allows remote attackers to	https://bugzilla.redhat.com/show_bug.cgi?id=1376646	A-RED-JBOSS--201016/198

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			cause a denial of service (CPU and disk consumption) via a long URL. **Reference: CVE-2016-7046**		
Denial of Service; Execute Code	2016-10-13	6.5	The JMX servlet in Red Hat JBoss Enterprise Application Platform (EAP) 4 and 5 allows remote authenticated users to cause a denial of service and possibly execute arbitrary code via a crafted serialized Java object. **Reference: CVE-2016-7065**	https://bugzilla.redhat.com/show_bug.cgi?id=1382534	A-RED-JBOSS--201016/199
S3-video Project					
S3-video NA					
Cross-site scripting	2016-10-12	4.3	Reflected XSS in wordpress plugin s3-video v0.983 **Reference: CVE-2016-1000148**	NA	A-S3--S3-VI--201016/200
SAP					
Netweaver SAP NetWeaver is the primary technology computing platform of the software company SAP SE, and the technical foundation for many SAP applications.					
Execute Code	2016-10-05	9	The (1) SCTC_REFRESH_EXPORT_TAB_COMP, (2) SCTC_REFRESH_CHECK_ENV, and (3) SCTC_TMS_MAINTAIN_ALOG functions in the SCTC subpackage in SAP Netweaver 7.40 SP 12 allow remote authenticated users with certain permissions to execute arbitrary commands via vectors involving a CALL 'SYSTEM' statement, aka SAP Security Note 2260344. **Reference: CVE-2016-7435**	NA	A-SAP-NETWE--201016/201
Siemens					
Automation License Manager The Automation License Manager (ALM) makes managing all your licenses especially efficient, and as easy as pie.					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

NA	2016-10-13	6.4	Siemens Automation License Manager (ALM) before 5.3 SP3 allows remote attackers to write to files, rename files, create directories, or delete directories via crafted packets. **Reference: CVE-2016-8565**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-284342.pdf	A-SIE-AUTOM--201016/202
Execute Code; SQL Injection	2016-10-13	6.4	SQL injection vulnerability in Siemens Automation License Manager (ALM) before 5.3 SP3 Update 1 allows remote attackers to execute arbitrary SQL commands via crafted traffic to TCP port 4410. **Reference: CVE-2016-8564**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-284342.pdf	A-SIE-AUTOM--201016/203
Denial of Service	2016-10-13	5	Siemens Automation License Manager (ALM) before 5.3 SP3 Update 1 allows remote attackers to cause a denial of service (ALM service outage) via crafted packets to TCP port 4410. **Reference: CVE-2016-8563**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-284342.pdf	A-SIE-AUTOM--201016/204
Simatic Step 7 STEP 7 basic software is the standard tool for the SIMATIC S7, SIMATIC C7 and SIMATIC WinAC automation systems. It enables the user to use the performance capability of these systems easily and conveniently.					
Gain Information	2016-10-13	1.9	Siemens SIMATIC STEP 7 (TIA Portal) before 14 uses an improper format for managing TIA project files during version updates, which makes it easier for local users to obtain sensitive configuration information via unspecified vectors. **Reference: CVE-2016-7960**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-869766.pdf	A-SIE-SIMAT--201016/205
Gain Information	2016-10-13	1.9	Siemens SIMATIC STEP 7 (TIA Portal) before 14 improperly stores pre-shared key data in TIA project files, which makes it easier for local users to obtain sensitive information	http://www.siemens.com/cert/pool/cert/siemens_security_adviso	A-SIE-SIMAT--201016/206

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			by leveraging access to a file and conducting a brute-force attack. **Reference: CVE-2016-7959**	ry_ssa-869766.pdf	
Simpel-reserveren Project					
Simpel-reserveren The software from Easy Reserve we make sure that website visitors are converted to guests.					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin simpel-reserveren v3.5.2 **Reference: CVE-2016-1000149**	NA	A-SIM-SIMPE--201016/207
Sophos					
Unified Threat Management Software Unified Threat Management Software has become established as a primary network gateway defense solution for organizations.UTM is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system, network firewalling, network intrusion detection/prevention (IDS/IPS), gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention, and on-appliance reporting.					
Gain Information	2016-10-04	2.1	The Frontend component in Sophos UTM with firmware 9.405-5 and earlier allows local administrators to obtain sensitive password information by reading the "value" field of the proxy user settings in "system settings / scan settings / anti spam" configuration tab. **Reference: CVE-2016-7442**	NA	A-SOP-UNIFI--201016/208
Gain Information	2016-10-04	2.1	The Frontend component in Sophos UTM with firmware 9.405-5 and earlier allows local administrators to obtain sensitive password information by reading the "value" field of the SMTP user settings in the notifications configuration tab. **Reference: CVE-2016-7397**	NA	A-SOP-UNIFI--201016/209
Tera-charts Project					
Tera Tera-charts scientific chart software gives you everything you need for publication quality chart plotting					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

in science and engineering.					
Cross-site scripting	2016-10-11	4.3	Reflected XSS in wordpress plugin tera-charts v1.0 **Reference: CVE-2016-1000151**	NA	A-TER-TERA--201016/210
Wptf-image-gallery Project					
Wptf-image-gallery WPTF is a WordPress plugin, using which an image gallery system can be built.					
NA	2016-10-07	5	Remote file download vulnerability in wptf-image-gallery v1.03 **Reference: CVE-2015-1000007**	http://www.vapidlabs.com/advisory.php?v=148	A-WPT-WPTF---201016/211
Zotpress Project					
Zotpress Zotpress brings zotero library and scholarly blogging to WordPress.					
SQL Injection	2016-10-07	7.5	Zotpress plugin for WordPress SQLi in zp_get_account() **Reference: CVE-2016-1000217**	NA	A-ZOT-ZOTPR--201016/212
Application; Operating System (A/OS)					
Adodb Project/Fedoraproject					
Adodb/Fedora Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project					
SQL Injection	2016-10-04	7.5	The qstr method in the PDO driver in the ADOdb Library for PHP before 5.x before 5.20.7 might allow remote attackers to conduct SQL injection attacks via vectors related to incorrect quoting. **Reference: CVE-2016-7405**	https://github.com/ADOdb/ADOdb/issues/226	A-ADO-ADODB--201016/213
C-ares Project/Debian					
C-ares/Debian Linux C-ares is a C library for asynchronous DNS requests; Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project.					
Denial of Service; Execute Code; Overflow	2016-10-03	7.5	Heap-based buffer overflow in the ares_create_query function in c-ares 1.x before 1.12.0 allows remote attackers to	https://googlechromereleases.blogspot.in/2016/	A-C-A-C-ARE--201016/214

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			cause a denial of service (out-of-bounds write) or possibly execute arbitrary code via a hostname with an escaped trailing dot. **Reference: CVE-2016-5180**	09/stable-channel-updates-for-chrome-os.html	
Eclipse/Fedora project					
Jetty/Fedora Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project.					
Gain Information	2016-10-11	5	The exception handling code in Eclipse Jetty before 9.2.9.v20150224 allows remote attackers to obtain sensitive information from process memory via illegal characters in an HTTP header, aka JetLeak. **Reference: CVE-2015-2080**	https://github.com/eclipse/jetty.project/blob/jetty-9.2.x/advisories/2015-02-24-httpparser-error-buffer-bleed.md	A-ECL-JETTY--201016/215
Freerdp Project/Novell					
Freerdp/Leap;Opensuse openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
Denial of Service	2016-10-04	5	FreeRDP before 1.1.0-beta1 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors. **Reference: CVE-2013-4118**	https://github.com/FreeRDP/FreeRDP/commit/7d58aac24fe20ffaad7bd9b40c9ddf457c1b06e7	A-FRE-FREER--201016/216
Haxx/Novell					
Libcurl/Leap libcurl is a free and easy-to-use client-side URL transfer library, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet and TFTP.					
NA	2016-10-04	5	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the	https://github.com/curl/curl/commit/curl-7_50_2~32	A-HAX-LIBCU--201016/217

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420. **Reference: CVE-2016-7141**		
Libgd/Novell					
Libgd/Leap; Opensuse GD is an open source code library for the dynamic creation of images by programmers;openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
Denial of Service	2016-10-04	4.3	The read_image_tga function in gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA image. **Reference: CVE-2016-6905**	https://github.com/libgd/libgd/commit/01c61f8ab110a77ae64b5ca67c244c728c506f03	A-LIB-LIBGD--201016/218
Libtiff/Novell					
Libtiff/Opensuse Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files. The set also contains command line tools for processing TIFFs;OpenSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
Denial of Service	2016-10-03	5	The rgb2ycbcr tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (divide-by-zero) by setting the (1) v or (2) h parameter to 0. **Reference: CVE-2016-3623**	http://bugzilla.maptools.org/show_bug.cgi?id=2569	A-LIB-LIBTI--201016/219
Nodejs/Suse					
Node.js/Linux Enterprise Node.js is available from the NodeSource Enterprise Linux and Fedora binary distributions repository/Linux Enterprise is designed for servers, mainframes, and workstations but can be installed on desktop computers for testing as well.					
NA	2016-10-12	4.3	The tls.checkServerIdentity function in Node.js 0.10.x before 0.10.47, 0.12.x before	https://nodejs.org/en/blog/vulnera	A-NOD-NODE.--201016/220

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			0.12.16, 4.x before 4.6.0, and 6.x before 6.7.0 does not properly handle wildcards in name fields of X.509 certificates, which allows man-in-the-middle attackers to spoof servers via a crafted certificate. **Reference: CVE-2016-7099**	bility/septe mber-2016-security-releases/	
Http R.Spl.	2016-10-12	4.3	CRLF injection vulnerability in the ServerResponse#writeHead function in Node.js 0.10.x before 0.10.47, 0.12.x before 0.12.16, 4.x before 4.6.0, and 6.x before 6.7.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the reason argument. **Reference: CVE-2016-5325**	https://nod ejs.org/en/b log/vulnera bility/septe mber-2016-security-releases/	A-NOD-NODE.--201016/221
Canonical;Debian/Djangoproject					
Ubuntu Linux/Debian Linux/Django Ubuntu is completely free to download, use and share.					
Bypass CSRF	2016-10-04	5	The cookie parsing code in Django before 1.8.15 and 1.9.x before 1.9.10, when used on a site with Google Analytics, allows remote attackers to bypass an intended CSRF protection mechanism by setting arbitrary cookies. **Reference: CVE-2016-7401**	https://ww w.djangopro ject.com/we blog/2016/s ep/26/secur ity-releases/	A-CAN-UBUNT--201016/222
Canonical;Novell/Gnome					
Ubuntu Linux/Leap;Opensuse/Gdk Ubuntu is completely free to download, use and share;openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
Denial of Service	2016-10-04	5	The OneLine32 function in io-ico.c in gdk-pixbuf before 2.35.3 allows remote attackers to cause a denial of service	https://git.g nome.org/br owse/gdk-pixbuf/tree/	A-CAN-UBUNT--201016/223

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			(out-of-bounds write and crash) via crafted dimensions in an ICO file. **Reference: CVE-2016-6352**	NEWS?id=640134c46221689d263369872937192e4484c83b	
Canonical/Clamav					
Ubuntu Linux/Clamav Ubuntu is completely free to download, use and share.					
Denial of Service	2016-10-04	4.3	ClamAV (aka Clam AntiVirus) before 0.99.2 allows remote attackers to cause a denial of service (application crash) via a crafted 7z file. **Reference: CVE-2016-1372**	https://bugzilla.clamav.net/show_bug.cgi?id=11514	A-CAN-UBUNT--201016/224
Denial of Service	2016-10-04	4.3	ClamAV (aka Clam AntiVirus) before 0.99.2 allows remote attackers to cause a denial of service (application crash) via a crafted mew packer executable. **Reference: CVE-2016-1371**	https://bugzilla.clamav.net/show_bug.cgi?id=11514	A-CAN-UBUNT--201016/225
Canonical/Systemd Project					
Ubuntu Linux/Systemd Ubuntu is completely free to download, use and share.					
Denial of Service	2016-10-13	4.9	The manager_invoke_notify_message function in systemd 231 and earlier allows local users to cause a denial of service (assertion failure and PID 1 hang) via a zero-length message received over a notify socket. **Reference: CVE-2016-7795**	https://github.com/systemd/systemd/issues/4234	A-CAN-UBUNT--201016/226
Debian/Libav					
Debian Linux/Libav Debian is an operating system and a distribution of Free Software/ Drupal is a scalable, open platform for web content management and digital experiences.					
Denial of Service	2016-10-11	4.3	The put_no_rnd_pixels8_xy2_mmx function in x86/rnd_template.c in libav 11.7 and earlier allows remote attackers to cause a	https://git.libav.org/?p=libav.git;a=commit;h=136f55207521f	A-DEB-DEBIA--201016/227

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			denial of service (NULL pointer dereference and crash) via a crafted MP3 file. **Reference: CVE-2016-7424**	0b03194ef5b55ba70f1635d6aee	
Debian/Perl					
Debian Linux/Perl Debian is an operating system and a distribution of Free Software/ Drupal is a scalable, open platform for web content management and digital experiences.					
Denial of Service; Overflow	2016-10-05	5	Buffer overflow in the DBD::mysql module before 4.037 for Perl allows context-dependent attackers to cause a denial of service (crash) via vectors related to an error message. **Reference: CVE-2016-1246**	https://github.com/perl5-dbi/DBD-mysql/commit/7c164a0c86cec6ee95df1d141e67b0e85dfdefd2	A-DEB-DEBIA--201016/228
Debian/Unadf Project					
Debian Linux/Unadf Debian is an operating system and a distribution of Free Software/ Drupal is a scalable, open platform for web content management and digital experiences.					
Execute Code	2016-10-04	9.3	The extractTree function in unADF allows remote attackers to execute arbitrary code via shell metacharacters in a directory name in an adf file. **Reference: CVE-2016-1244**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=838248	A-DEB-DEBIA--201016/229
Execute Code; Overflow	2016-10-04	7.5	Stack-based buffer overflow in the extractTree function in unADF allows remote attackers to execute arbitrary code via a long pathname. **Reference: CVE-2016-1243**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=838248	A-DEB-DEBIA--201016/230
Fedoraproject;Novell/GNU					
Fedora/Opensuse/Glibc Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project;openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
Denial of Service	2016-10-11	5	The makecontext function in the GNU C Library (aka glibc or libc6) before 2.25 creates execution contexts	https://sourceware.org/bugzilla/show_bug.cgi?id	A-FED-FEDOR--201016/231

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			incompatible with the unwinder on ARM EABI (32-bit) platforms, which might allow context-dependent attackers to cause a denial of service (hang), as demonstrated by applications compiled using gccgo, related to backtrace generation. **Reference: CVE-2016-6323**	=20435	
Fedoraproject/Haxx					
Fedora/Libcurl Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project.					
Overflow	2016-10-11	7.5	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow. **Reference: CVE-2016-7167**	https://curl.haxx.se/docs/adv_20160914.html	A-FED-FEDOR--201016/232
Fedoraproject/Mongodb					
Fedora/Mongodb Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project.					
Gain Information	2016-10-04	2.1	The client in MongoDB uses world-readable permissions on .dbshell history files, which might allow local users to obtain sensitive information by reading these files. **Reference: CVE-2016-6494**	https://github.com/mongodb/mongo/commit/035cf2afc04988b22cb67f4ebfd77e9b344cb6e0	A-FED-FEDOR--201016/233
Linux;Redhat/Redhat					
Linux Kernel/Linux/Enterprise Mrg The Linux kernel is a Unix-like computer operating system kernel.					
Execute Code;Bypass	2016-10-11	6.9	The Linux kernel, as used in Red Hat Enterprise Linux 7.2 and Red Hat Enterprise MRG 2	https://bugzilla.redhat.com/show_bu	A-LIN-LINUX--201016/234

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			and when booted with UEFI Secure Boot enabled, allows local users to bypass intended Secure Boot restrictions and execute untrusted code by appending ACPI tables to the initrd. **Reference: CVE-2016-3699**	g.cgi?id=1329653	
Novell;Redhat/Systemd Project					
Suse Linux Enterprise Desktop;Suse Linux Enterprise Server;Suse Linux Enterprise Server For Sap;Suse Linux Enterprise Software Development Kit/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation/Systemd SUSE Linux Enterprise Desktop delivers essential office functionality affordably, and was built to coexist with other operating systems; SUSE Linux Enterprise Server for SAP Applications based on SUSE Linux Enterprise 12, the reliable, scalable and secure platform for efficiently deploying and managing highly available enterprise-class IT services in physical, virtual or cloud infrastructure. SUSE Linux Enterprise Software Development Kit is a comprehensive development tool kit that is designed to support developers, as well as independent hardware vendors (IHVs) and independent software vendors (ISVs), in creating applications on or porting them to SUSE Linux Enterprise products.					
Denial of Service	2016-10-13	4.9	The manager_dispatch_notify_fd function in systemd allows local users to cause a denial of service (system hang) via a zero-length message received over a notify socket, which causes an error to be returned and the notification handler to be disabled. **Reference: CVE-2016-7796**	https://bugzilla.redhat.com/show_bug.cgi?id=1381911	A-NOV-SUSE--201016/235
Novell/Openjpeg					
Openjpeg/Leap OpenJPEG is an open-source JPEG 2000 codec written in C language.					
Denial of Service	2016-10-03	5	convert.c in OpenJPEG before 2.1.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors involving the variable s. **Reference: CVE-2016-7445**	https://github.com/uclouvain/openjpeg/blob/openjpeg-2.1/CHANGELOG.md	A-NOV-OPENJ--201016/236
Operating System (OS)					
Animas					
Onetouch Ping Firmware					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

The OneTouch Ping gives a meter-remote that controls pump functions from up to 10 feet (3.0 metres) away. The pump and meter-remote communicate and share information wirelessly, so you can keep your pump under cover.					
Bypass	2016-10-05	9.3	Johnson & Johnson Animas OneTouch Ping devices allow remote attackers to bypass authentication via replay attacks. **Reference: CVE-2016-5086**	NA	O-ANI-ONETO--201016/237
Gain Information	2016-10-05	5	Johnson & Johnson Animas OneTouch Ping devices do not use encryption for certain data, which might allow remote attackers to obtain sensitive information by sniffing the network. **Reference: CVE-2016-5084**	NA	O-ANI-ONETO--201016/238
Bypass	2016-10-07	9.3	Johnson & Johnson Animas OneTouch Ping devices mishandle acknowledgements, which makes it easier for remote attackers to bypass authentication via a custom communication protocol. **Reference: CVE-2016-5686**	NA	O-ANI-ONETO--201016/239
Canonical;Debian;Linux					
Ubuntu Linux/Debian Linux/Linux Kernel The Linux kernel is a Unix-like computer operating system kernel.					
Execute Code	2016-10-12	10	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing. **Reference: CVE-2016-7117**	https://people.canonical.com/~ubuntu-security/cve/2016/CVE-2016-7117.html	O-CAN-UBUNT--201016/240
Cisco					
IOS Cisco IOS is network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware platform support.					
Denial of Service	2016-10-06	6.3	The IKEv2 client and initiator	http://tools.	O-CIS-IOS--

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			implementations in Cisco IOS 15.5(3)M and IOS XE allow remote IKEv2 servers to cause a denial of service (device reload) via crafted IKEv2 packets, aka Bug ID CSCux97540. **Reference: CVE-2016-6423**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ios-ikev	201016/241
Bypass	2016-10-06	4.3	Cisco IOS 12.2(33)SXJ9 on Supervisor Engine 32 and 720 modules for 6500 and 7600 devices mishandles certain operators, flags, and keywords in TCAM share ACLs, which allows remote attackers to bypass intended access restrictions by sending packets that should have been recognized by a filter, aka Bug ID CSCuy64806. **Reference: CVE-2016-6422**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-catalyst	O-CIS-IOS--201016/242
Denial of Service	2016-10-06	7.1	The AAA service in Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.1 through 3.18 and 16.2 allows remote attackers to cause a denial of service (device reload) via a failed SSH connection attempt that is mishandled during generation of an error-log message, aka Bug ID CSCuy87667. **Reference: CVE-2016-6393**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-aaados	O-CIS-IOS--201016/243
Denial of Service	2016-10-06	7.8	Cisco IOS 12.2 and 15.0 through 15.3 allows remote attackers to cause a denial of service (traffic-processing outage) via a crafted series of Common Industrial Protocol (CIP) requests, aka Bug ID CSCur69036. **Reference: CVE-2016-6391**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-cip	O-CIS-IOS--201016/244
Denial of Service	2016-10-06	7.8	Cisco IOS 12.2 through 12.4 and 15.0 through 15.6 and IOS	http://tools.cisco.com/se	O-CIS-IOS--201016/245

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			XE 3.1 through 3.17 and 16.2 allow remote attackers to cause a denial of service (device reload) via crafted fields in an H.323 message, aka Bug ID CSCux04257. **Reference: CVE-2016-6384**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-h323	
Denial of Service; Memory Corruption ; Gain Information	2016-10-06	8.3	The DNS forwarder in Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 3.1 through 3.15 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (data corruption or device reload) via a crafted DNS response, aka Bug ID CSCup90532. **Reference: CVE-2016-6380**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-dns	O-CIS-IOS--201016/246
Ios Xe IOS XE represents the continuing evolution of Cisco's pre-eminent IOS operating system. IOS XE is architected for routers, switches and appliances.					
Denial of Service	2016-10-06	7.8	Cisco IOS XE 3.1 through 3.17 and 16.1 through 16.2 allows remote attackers to cause a denial of service (device reload) via crafted ICMP packets that require NAT, aka Bug ID CSCuw85853. **Reference: CVE-2016-6378**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-esp-nat	O-CIS-IOS X--201016/247
Ios Xe;Ios Xe 16.1;Ios Xe 3.1sg;Ios Xe 3.2ja;Ios Xe 3.2sg;Ios Xe 3.2xo;Ios Xe 3.3sg;Ios Xe 3.3sq;Ios Xe 3.3xo;Ios Xe 3.4sg;Ios Xe 3.4sq;Ios Xe 3.5sq;Ios Xe 3.8ex IOS XE represents the continuing evolution of Cisco's pre-eminent IOS operating system. IOS XE is architected for routers, switches and appliances.					
Denial of Service	2016-10-05	7.8	Cisco IOS XE 3.1 through 3.17 and 16.1 on 64-bit platforms allows remote attackers to cause a denial of service (data-structure corruption and device reload) via fragmented IPv4 packets, aka Bug ID CSCux66005. **Reference: CVE-2016-6386**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-frag	O-CIS-IOS X--201016/248

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Ios Xr IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end Network Converging System (NCS), carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series.					
Execute Code	2016-10-06	7.2	Cisco IOS XR 6.1.1 allows local users to execute arbitrary OS commands as root by leveraging admin privileges, aka Bug ID CSCva38349. **Reference: CVE-2016-6428**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-iosxr	O-CIS-IOS X--201016/249
Denial of Service	2016-10-06	5	Cisco IOS XR 5.2.2 allows remote attackers to cause a denial of service (process restart) via a crafted OSPF Link State Advertisement (LSA) update, aka Bug ID CSCvb05643. **Reference: CVE-2016-6421**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ospf	O-CIS-IOS X--201016/250
IOS;Ios Xe Cisco IOS is network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware platform support.					
Denial of Service	2016-10-06	7.8	Memory leak in the Smart Install client implementation in Cisco IOS 12.2 and 15.0 through 15.2 and IOS XE 3.2 through 3.8 allows remote attackers to cause a denial of service (memory consumption) via crafted image-list parameters, aka Bug ID CSCuy82367. **Reference: CVE-2016-6385**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-smi	O-CIS-IOS;I--201016/251
Denial of Service	2016-10-06	7.8	Cisco IOS 15.2 through 15.6 and IOS XE 3.6 through 3.17 and 16.1 allow remote attackers to cause a denial of service (device restart) via a malformed IPv6 Protocol Independent Multicast (PIM) register packet, aka Bug ID	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-	O-CIS-IOS;I--201016/252

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CSCuy16399. **Reference: CVE-2016-6382**	msdp	
Denial of Service	2016-10-06	7.8	Cisco IOS 12.2 and IOS XE 3.14 through 3.16 and 16.1 allow remote attackers to cause a denial of service (device reload) via crafted IP Detail Record (IPDR) packets, aka Bug ID CSCuu35089. **Reference: CVE-2016-6379**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ipdr	O-CIS-IOS;I--201016/253
IOS;Ios Xe;Ios Xe 16.1;Ios Xe 3.3sg;Ios Xe 3.3xo Cisco IOS is network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware platform support.					
Denial of Service	2016-10-05	7.1	Cisco IOS 12.4 and 15.0 through 15.6 and IOS XE 3.1 through 3.18 and 16.1 allow remote attackers to cause a denial of service (memory consumption or device reload) via fragmented IKEv1 packets, aka Bug ID CSCuy47382. **Reference: CVE-2016-6381**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ios-ikev1	O-CIS-IOS;I--201016/254
IOS;Ios Xe;Ios Xe 3.2ja;Ios Xe 3.3sg;Ios Xe 3.3xo;Ios Xe 3.4sg Cisco IOS is network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware platform support.					
Denial of Service	2016-10-05	7.8	Cisco IOS 12.2 and 15.0 through 15.3 and IOS XE 3.1 through 3.9 allow remote attackers to cause a denial of service (device restart) via a crafted IPv4 Multicast Source Discovery Protocol (MSDP) Source-Active (SA) message, aka Bug ID CSCud36767. **Reference: CVE-2016-6392**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-msdp	O-CIS-IOS;I--201016/255
Nx-os Cisco NX-OS operating system delivers industry-leading innovations that reduce data center network complexity and cost, and increase efficiency.					
Denial of Service	2016-10-07	7.8	Cisco NX-OS 4.1 through 7.3 and 11.0 through 11.2 on Nexus 2000, 3000, 3500, 5000, 5500, 5600, 6000, 7000, 7700, and 9000 devices allows	http://tools.cisco.com/security/center/content/CiscoSecurityA	O-CIS-NX-OS--201016/256

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			remote attackers to cause a denial of service (device crash) via malformed IPv4 DHCP packets to the DHCPv4 relay agent, aka Bug IDs CSCuq39250, CSCus21733, CSCus21739, CSCut76171, and CSCux67182. **Reference: CVE-2015-6393**	dvisory/cisco-sa-20161005-dhcp2	
Bypass	2016-10-12	9	Cisco NX-OS 4.0 through 7.3 on Multilayer Director and Nexus 1000V, 2000, 3000, 3500, 4000, 5000, 5500, 5600, 6000, 7000, 7700, and 9000 devices allows remote authenticated users to bypass intended AAA restrictions and obtain privileged CLI access via crafted parameters in an SSH connection negotiation, aka Bug IDs CSCum35502, CSCuw78669, CSCuw79754, and CSCux88492. **Reference: CVE-2015-0721**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-nxaaa	O-CIS-NX-OS--201016/257
Denial of Service	2016-10-13	7.1	Cisco NX-OS 4.0 through 7.3 and 11.0 through 11.2 on 1000v, 2000, 3000, 3500, 5000, 5500, 5600, 6000, 7000, 7700, and 9000 devices allows remote attackers to cause a denial of service (device reload) by leveraging a peer relationship to send a crafted BGP UPDATE message, aka Bug IDs CSCuq77105 and CSCux11417. **Reference: CVE-2016-1454**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-bgp	O-CIS-NX-OS--201016/258
Denial of Service	2016-10-13	7.8	Cisco NX-OS 4.1 through 7.2 on Nexus 2000, 5000, 5500, 5600, 6000, 7000, 7700, and 9000 devices allows remote attackers to cause a denial of service (device crash) via crafted IPv4 DHCP packets to	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-NX-OS--201016/259

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			the (1) DHCPv4 relay agent or (2) smart relay agent, aka Bug IDs CSCuq24603, CSCur93159, CSCus21693, and CSCut76171. **Reference: CVE-2015-6392**	20161005-dhcp1	
Fortinet					
Fortianalyzer Firmware;Fortimanager Firmware FortiManager offers the features to contain threats as well as providing flexibility to evolve along with your ever-changing network. FortiManager enterprise-class features deliver: The flexiblity to manage just a few or thousands of FortiGate devices.					
Cross-site scripting	2016-10-11	3.5	Cross-site scripting (XSS) vulnerability in the advanced settings page in Fortinet FortiManager 5.x before 5.0.12 and 5.2.x before 5.2.3, in hardware models with a hard disk, and FortiAnalyzer 5.x before 5.0.13 and 5.2.x before 5.2.3 allows remote administrators to inject arbitrary web script or HTML via vectors related to report filters. **Reference: CVE-2015-7363**	http://fortiguard.com/advisory/fortianalyzer-and-fortimanager-stored-xss-vulnerability-in-report-filters	O-FOR-FORTI--201016/260
Google					
Android Android (from its former owner Android, Inc.) is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smart phones and tablets.					
Denial of Service; Overflow	2016-10-11	7.5	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted visualizer data length, aka Qualcomm internal bug CR 1033540. **Reference: CVE-2016-6695**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/261
Gain Information	2016-10-11	4.3	Binder in the kernel in Android before 2016-10-05 on Nexus devices allows attackers to	http://source.android.com/security/	O-GOO-ANDRO--201016/262

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			obtain sensitive information via a crafted application, aka internal bug 30768347. **Reference: CVE-2016-6689**	bulletin/2016-10-01.html	
Gain Information	2016-10-11	4.3	The NVIDIA profiler in Android before 2016-10-05 on Nexus 9 devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 30593080. **Reference: CVE-2016-6688**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/263
Gain Information	2016-10-11	4.3	The NVIDIA profiler in Android before 2016-10-05 on Nexus 9 devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 30162222. **Reference: CVE-2016-6687**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/264
Gain Information	2016-10-11	4.3	The kernel in Android before 2016-10-05 on Nexus 6P devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 30402628. **Reference: CVE-2016-6685**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/265
Gain Information	2016-10-11	4.3	The kernel in Android before 2016-10-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Nexus Player, and Android One devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 30148243. **Reference: CVE-2016-6684**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/266
Gain Information	2016-10-11	4.3	The kernel in Android before 2016-10-05 on Nexus devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 30143283. **Reference: CVE-2016-6683**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/267
Gain Information	2016-10-11	6.8	CORE/HDD/src/wlan_hdd_wext.c in the Qualcomm Wi-Fi driver in Android before 2016-	http://source.android.com/security/	O-GOO-ANDRO--201016/268

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			10-05 on Nexus 5X and Android One devices allows attackers to obtain sensitive information via a crafted application that makes an iw_set_priv ioctl call, aka Android internal bug 29982678 and Qualcomm internal bug CR 1048052. **Reference: CVE-2016-6680**	bulletin/2016-10-01.html	
Gain Information	2016-10-11	4.3	The Motorola USBNet driver in Android before 2016-10-05 on Nexus 6 devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 29914434. **Reference: CVE-2016-6678**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/269
Gain Information	2016-10-11	4.3	The NVIDIA GPU driver in Android before 2016-10-05 on Nexus 9 devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 30259955. **Reference: CVE-2016-6677**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/270
Denial of Service;Overflow; Gain Privileges	2016-10-11	9.3	Off-by-one error in CORE/HDD/src/wlan_hdd_cfg.c in the Qualcomm Wi-Fi driver in Android before 2016-10-05 on Nexus 5X and Android One devices allows attackers to gain privileges or cause a denial of service (buffer overflow) via a crafted application that makes a GET_CFG ioctl call, aka Android internal bug 30874066 and Qualcomm internal bug CR 1000853. **Reference: CVE-2016-6676**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/271
Gain Privileges	2016-10-11	6.8	system_server in Android before 2016-10-05 on Nexus devices allows attackers to	http://source.android.com/security/	O-GOO-ANDRO--201016/272

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			gain privileges via a crafted application, aka internal bug 30445380. **Reference: CVE-2016-6674**	bulletin/2016-10-01.html	
Gain Privileges	2016-10-11	9.3	The Synaptics touchscreen driver in Android before 2016-10-05 on Nexus 5X devices allows attackers to gain privileges via a crafted application, aka internal bug 30537088. **Reference: CVE-2016-6672**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/273
Gain Privileges	2016-10-11	9.3	The MediaTek video driver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 30030994 and MediaTek internal bug ALPS02834874. **Reference: CVE-2016-3937**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/274
Gain Privileges	2016-10-11	9.3	The MediaTek video driver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 30019037 and MediaTek internal bug ALPS02829568. **Reference: CVE-2016-3936**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/275
Overflow; Gain Privileges	2016-10-11	9.3	drivers/media/platform/msm/camera_v2/sensor/io/msm_camera_cci_i2c.c in the Qualcomm camera driver in Android before 2016-10-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Android One devices relies on variable-length arrays, which allows attackers to gain privileges via a crafted application, aka Android internal bug 30102557 and Qualcomm internal bug CR 789704.	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/276

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-3934		
Gain Privileges	2016-10-11	9.3	The NVIDIA MMC test driver in Android before 2016-10-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28760138. **Reference: CVE-2016-3930**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/277
Gain Privileges	2016-10-11	9.3	The MediaTek video driver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 30019362 and MediaTek internal bug ALPS02829384. **Reference: CVE-2016-3928**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/278
Gain Privileges	2016-10-11	4.3	The Accessibility services in Android 7.0 before 2016-10-01 mishandle motion events, which allows attackers to conduct touchjacking attacks and consequently gain privileges via a crafted application, aka internal bug 30647115. **Reference: CVE-2016-3923**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/279
Gain Privileges	2016-10-11	6.8	libril/RilSapSocket.cpp in Telephony in Android 6.x before 2016-10-01 and 7.0 before 2016-10-01 relies on variable-length arrays, which allows attackers to gain privileges via a crafted application, aka internal bug 30202619. **Reference: CVE-2016-3922**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/280
Gain Information	2016-10-11	4.3	email/provider/AttachmentProvider.java in AOSP Mail in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 does not	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/281

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			ensure that certain values are integers, which allows attackers to read arbitrary attachments via a crafted application that provides a pathname value, aka internal bug 30745403. **Reference: CVE-2016-3918**		
Gain Privileges	2016-10-11	9.3	Race condition in providers/telephony/MmsProvider.java in Telephony in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application that modifies a database between two open operations, aka internal bug 30481342. **Reference: CVE-2016-3914**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/282
Gain Privileges	2016-10-11	9.3	CORE/HDD/src/wlan_hdd_main.c in the Qualcomm Wi-Fi driver in Android before 2016-10-05 on Nexus 5X devices allows attackers to gain privileges via a crafted application that sends a SENDACTIONFRAME command, aka Android internal bug 28061823 and Qualcomm internal bug CR 1001449. **Reference: CVE-2016-3905**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/283
Gain Privileges	2016-10-11	9.3	drivers/media/platform/msm/camera_v2/sensor/csid/msm_csid.c in the Qualcomm camera driver in Android before 2016-10-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/284

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			internal bug 29513227 and Qualcomm internal bug CR 1040857. **Reference: CVE-2016-3903**		
Gain Information	2016-10-11	4.3	drivers/platform/msm/ipa/ipa_qmi_service.c in the Qualcomm IPA driver in Android before 2016-10-05 on Nexus 5X and 6P devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 29953313 and Qualcomm internal bug CR 1044072. **Reference: CVE-2016-3902**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/285
Overflow; Gain Privileges	2016-10-11	9.3	Multiple integer overflows in drivers/crypto/msm/qcedev.c in the Qualcomm cryptographic engine driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29999161 and Qualcomm internal bug CR 1046434. **Reference: CVE-2016-3901**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/286
Gain Privileges	2016-10-11	9.3	cmds/servicemanager/service_manager.c in ServiceManager in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 does not properly restrict service registration, which allows attackers to gain privileges via a crafted application, aka internal bug 29431260. **Reference: CVE-2016-3900**	https://android.googlesource.com/platform/frameworks/native/+/047eec456943dc082e33220d28abb7df4e089f69	O-GOO-ANDRO--201016/287
Denial of Service	2016-10-11	6.1	Off-by-one error in server/wifi/anqp/VenueNameElement.java in Wi-Fi in	http://source.android.com/security/	O-GOO-ANDRO--201016/288

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Android 6.x before 2016-10-01 and 7.0 before 2016-10-01 allows remote attackers to cause a denial of service (reboot) via an access point that provides a crafted (1) Venue Group or (2) Venue Type value, aka internal bug 29464811. **Reference: CVE-2016-3882**	bulletin/2016-10-01.html	
Gain Information	2016-10-11	4.3	sound/soc/msm/qdsp6v2/audio_calibration.c in the Qualcomm sound driver in Android before 2016-10-05 on Nexus 5X, Nexus 6P, and Android One devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 29323142 and Qualcomm internal bug CR 1038127. **Reference: CVE-2016-3860**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/289
Gain Privileges	2016-10-11	9.3	Multiple use-after-free vulnerabilities in sound/soc/msm/qdsp6v2/msm-lsm-client.c in the Qualcomm sound driver in Android before 2016-10-05 on Nexus 5X, Nexus 6P, and Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 30142668 and Qualcomm internal bug CR 948902. **Reference: CVE-2015-8951**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/290
Denial of Service	2016-10-12	7.5	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/291

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			via a large negative value for the data length, aka Qualcomm internal bug CR 1041130. **Reference: CVE-2016-6696**		
Denial of Service	2016-10-12	7.5	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact via crafted parameter data, aka Qualcomm internal bug CR 1033525. **Reference: CVE-2016-6694**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/292
Denial of Service	2016-10-12	7.5	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact via an invalid data length, aka Qualcomm internal bug CR 1027585. **Reference: CVE-2016-6693**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/293
Denial of Service	2016-10-12	7.5	drivers/video/msm/mdss/mdss_mdp_pp.c in the Qualcomm MDSS driver in Android before 2016-10-05 allows attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via unknown vectors, aka Qualcomm internal bug CR 1004933. **Reference: CVE-2016-6692**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/294
Denial of Service	2016-10-12	7.5	service/jni/com_android_server_wifi_Gbk2Utf.cpp in the Qualcomm Wi-Fi gbk2utf module in Android before 2016-10-05 allows remote attackers to cause a denial of service (framework crash) or	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/295

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			possibly have unspecified other impact via an access point that has a malformed SSID with GBK encoding, aka Qualcomm internal bug CR 978452. **Reference: CVE-2016-6691**		
Denial of Service	2016-10-12	7.1	The sound driver in the kernel in Android before 2016-10-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Nexus Player devices allows attackers to cause a denial of service (reboot) via a crafted application, aka internal bug 28838221. **Reference: CVE-2016-6690**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/296
Gain Information	2016-10-12	4.3	The NVIDIA profiler in Android before 2016-10-05 on Nexus 9 devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 30163101. **Reference: CVE-2016-6686**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/297
Gain Information	2016-10-12	4.3	drivers/misc/qcom/qdsp6v2/audio_utils.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 on Nexus 5X, Nexus 6P, and Android One devices does not initialize certain data structures, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 30152501 and Qualcomm internal bug CR 1049615. **Reference: CVE-2016-6682**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/298
Gain Information	2016-10-12	4.3	drivers/misc/qcom/qdsp6v2/audio_utils.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 on Nexus 5X, Nexus 6P, and Android One devices does not initialize	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/299

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			certain data structures, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 30152182 and Qualcomm internal bug CR 1049521. **Reference: CVE-2016-6681**		
Gain Information	2016-10-12	4.3	CORE/HDD/src/wlan_hdd_hostapd.c in the Qualcomm Wi-Fi driver in Android before 2016-10-05 on Nexus 5X and Android One devices allows attackers to obtain sensitive information via a crafted application that makes a setwpaie ioctl call, aka Android internal bug 29915601 and Qualcomm internal bug CR 1000913. **Reference: CVE-2016-6679**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/300
Denial of Service; Overflow; Gain Privileges	2016-10-12	9.3	Off-by-one error in CORE/HDD/src/wlan_hdd_hostapd.c in the Qualcomm Wi-Fi driver in Android before 2016-10-05 on Nexus 5X and Android One devices allows attackers to gain privileges or cause a denial of service (buffer overflow) via a crafted application that makes a linkspeed ioctl call, aka Android internal bug 30873776 and Qualcomm internal bug CR 1000861. **Reference: CVE-2016-6675**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/301
Gain Privileges	2016-10-12	9.3	The NVIDIA camera driver in Android before 2016-10-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 30204201. **Reference: CVE-2016-6673**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/302

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service	2016-10-12	7.1	The GPS component in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows man-in-the-middle attackers to cause a denial of service (memory consumption, and device hang or reboot) via a large xtra.bin or xtra2.bin file on a spoofed Qualcomm gpsonextra.net or izatcloud.net host, aka internal bug 29555864. **Reference: CVE-2016-5348**	https://code.google.com/p/android/issues/detail?id=213747	O-GOO-ANDRO--201016/303
Gain Privileges	2016-10-12	9.3	The Synaptics touchscreen driver in Android before 2016-10-05 on Nexus 6P and Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 30141991. **Reference: CVE-2016-3940**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/304
Gain Privileges	2016-10-12	9.3	drivers/video/msm/mdss/mdss_debug.c in the Qualcomm video driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 30874196 and Qualcomm internal bug CR 1001224. **Reference: CVE-2016-3939**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/305
Gain Privileges	2016-10-12	9.3	drivers/video/msm/mdss/mdss_mdp_overlay.c in the Qualcomm video driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/306

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			internal bug 30019716 and Qualcomm internal bug CR 1049232. **Reference: CVE-2016-3938**		
Overflow; Gain Privileges	2016-10-12	9.3	Multiple integer overflows in drivers/crypto/msm/qcedev.c in the Qualcomm cryptographic engine driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29999665 and Qualcomm internal bug CR 1046507. **Reference: CVE-2016-3935**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/307
Gain Privileges	2016-10-12	9.3	mediaserver in Android before 2016-10-05 on Nexus 9 and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 29421408. **Reference: CVE-2016-3933**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/308
Gain Privileges	2016-10-12	9.3	mediaserver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 29161895 and MediaTek internal bug ALPS02770870. **Reference: CVE-2016-3932**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/309
Gain Privileges	2016-10-12	9.3	drivers/misc/qseecom.c in the Qualcomm QSEE Communicator driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 29157595 and Qualcomm internal bug CR 1036418.	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/310

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-3931		
NA	2016-10-12	10	Unspecified vulnerability in a Qualcomm component in Android before 2016-10-05 on Nexus 5X and 6P devices has unknown impact and attack vectors, aka internal bug 28823675. **Reference: CVE-2016-3929**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/311
NA	2016-10-12	10	Unspecified vulnerability in a Qualcomm component in Android before 2016-10-05 on Nexus 5X and 6P devices has unknown impact and attack vectors, aka internal bug 28823244. **Reference: CVE-2016-3927**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/312
NA	2016-10-12	10	Unspecified vulnerability in a Qualcomm component in Android before 2016-10-05 on Nexus 5, 5X, 6, and 6P devices has unknown impact and attack vectors, aka internal bug 28823953. **Reference: CVE-2016-3926**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/313
Denial of Service	2016-10-12	4.3	server/wifi/anqp/ANQPFactory.java in Android 6.x before 2016-10-01 and 7.0 before 2016-10-01 allows attackers to cause a denial of service (blocked Wi-Fi usage) via a crafted application, aka internal bug 30230534. **Reference: CVE-2016-3925**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/314
Gain Information	2016-10-12	4.3	services/audioflinger/Effects.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 does not validate EFFECT_CMD_SET_PARAM and EFFECT_CMD_SET_PARAM_DE	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/315

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			FERRED commands, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 30204301. **Reference: CVE-2016-3924**		
Gain Privileges	2016-10-12	9.3	libsysutils/src/FrameworkListener.cpp in Framework Listener in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 29831647. **Reference: CVE-2016-3921**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/316
Denial of Service	2016-10-12	7.1	id3/ID3.cpp in libstagefright in mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 30744884. **Reference: CVE-2016-3920**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/317
Overflow; Gain Privileges	2016-10-12	9.3	camera/src/camera_metadata.c in the Camera service in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30741779. **Reference: CVE-2016-3916**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/318
Gain Privileges	2016-10-12	9.3	camera/src/camera_metadata.c in the Camera service in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/319

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			a crafted application, aka internal bug 30591838. **Reference: CVE-2016-3915**		
Gain Privileges	2016-10-12	9.3	media/libmediaplayerservice/MediaPlayerService.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 does not validate a certain static_cast operation, which allows attackers to gain privileges via a crafted application, aka internal bug 30204103. **Reference: CVE-2016-3913**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/320
Gain Privileges	2016-10-12	9.3	The framework APIs in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allow attackers to gain privileges via a crafted application, aka internal bug 30202481. **Reference: CVE-2016-3912**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/321
Gain Privileges	2016-10-12	9.3	core/java/android/os/Process.java in Zygote in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30143607. **Reference: CVE-2016-3911**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/322
Gain Privileges	2016-10-12	9.3	services/soundtrigger/SoundTriggerHwService.cpp in mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30148546.	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/323

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Reference: CVE-2016-3910		
Gain Privileges	2016-10-12	9.3	The SoftMPEG4 component in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30033990. **Reference: CVE-2016-3909**	https://android.googlesource.com/platform/frameworks/av/+/d4271b792bdad85a80e2b83ab34c4b30b74f53ec	O-GOO-ANDRO--201016/324
Gain Privileges	2016-10-12	4.3	The Lock Settings Service in Android 6.x before 2016-10-01 and 7.0 before 2016-10-01 allows attackers to remove a device's PIN or password, and consequently gain privileges, via a crafted application, aka internal bug 30003944. **Reference: CVE-2016-3908**	http://source.android.com/security/bulletin/2016-10-01.html	O-GOO-ANDRO--201016/325
Google;Linux					
Android/Linux Kernel Android (from its former owner Android, Inc.) is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets;/The Linux kernel is a Unix-like computer operating system kernel.					
Denial of Service;Gain Information	2016-10-11	3.6	The rfcomm_sock_bind function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 4.2 allows local users to obtain sensitive information or cause a denial of service (NULL pointer dereference) via vectors involving a bind system call on a Bluetooth RFCOMM socket. **Reference: CVE-2015-8956**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=951b6a0717db97ce420547222647bcc40bf1eacd	O-GOO-ANDRO--201016/326
Denial of Service;Gain Privileges	2016-10-12	6.9	arch/arm64/kernel/perf_event.c in the Linux kernel before 4.1 on arm64 platforms allows local users to gain privileges or cause a denial of service	https://github.com/torvalds/linux/commit/8fff105e13041e4	O-GOO-ANDRO--201016/327

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			(invalid pointer dereference) via vectors involving events that are mishandled during a span of multiple HW PMUs. **Reference: CVE-2015-8955**	9b82f92eef034f363a6b1c071	
Huawei					
Ar Firmware;Quidway S5300 Firmware;Quidway S9300 Firmware;S12700 Firmware;S5300 Firmware;S5700 Firmware;S9300 Firmware NA					
NA	2016-10-04	4	Huawei AR routers with software before V200R007C00SPC100; Quidway S9300 routers with software before V200R009C00; S12700 routers with software before V200R008C00SPC500; S9300, Quidway S5300, and S5300 routers with software before V200R007C00; and S5700 routers with software before V200R007C00SPC500 makes it easier for remote authenticated administrators to obtain encryption keys and ciphertext passwords via vectors related to key storage. **Reference: CVE-2015-8086**	http://www.huawei.com/en/psirt/security-advisories/hw-455876	O-HUA-ARFI--201016/328
Ar Firmware;Quidway S5300 Firmware;Quidway S9300 Firmware;S12700 Firmware;S5300 Firmware;S5700 Firmware;S9300 Firmware NA					
NA	2016-10-04	4	Huawei AR routers with software before V200R007C00SPC100; Quidway S9300 routers with software before V200R009C00; S12700 routers with software before V200R008C00SPC500; S9300, Quidway S5300, and S5300 routers with software before V200R007C00; and S5700 routers with software before V200R007C00SPC500 make it	http://www.huawei.com/en/psirt/security-advisories/hw-455876	O-HUA-ARFI--201016/329

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			easier for remote authenticated administrators to obtain and decrypt passwords by leveraging selection of a reversible encryption algorithm. **Reference: CVE-2015-8085**		
Linux					
Linux Kernel The Linux kernel is a Unix-like computer operating system kernel.					
Denial of Service; Overflow; Memory Corruption.	2016-10-12	7.5	drivers/soc/qcom/qdsp6v2/voice_svc.c in the QDSP6v2 Voice Service driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a write request, as demonstrated by a voice_svc_send_req buffer overflow. **Reference: CVE-2016-5343**	http://source.android.com/security/bulletin/2016-10-01.html	O-LIN-LINUX--201016/330
Gain Information	2016-10-12	4.3	arch/arm64/mm/dma-mapping.c in the Linux kernel before 4.0.3, as used in the ION subsystem in Android and other products, does not initialize certain data structures, which allows local users to obtain sensitive information from kernel memory by triggering a dma_mmap call. **Reference: CVE-2015-8950**	https://github.com/torvalds/linux/commit/6829e274a623187c24f7cfc0e3d35f25d087fcc5	O-LIN-LINUX--201016/331
Denial of Service	2016-10-12	7.5	Multiple race conditions in drivers/char/adsprpc.c and drivers/char/adsprpc_compat.c in the ADSPRPC driver for the Linux kernel 3.x, as used in	https://source.codeaurora.org/quic/la/kernel/msm/commit/?	O-LIN-LINUX--201016/332

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service (zero-value write) or possibly have unspecified other impact via a COMPAT_FASTRPC_IOCTL_INVOKE_FD ioctl call. **Reference: CVE-2015-0572**	id=8fb32c3a8147b82e2bb159b3f70d803c9e68899b	
XEN					
XEN Xen Project: Open Source Hypervisor, High Performance Clouds, Free Software, Open Source Virtualization, Open Virtualization, Cloud Computing, Desktop.					
NA	2016-10-11	3.3	Xen 4.7.x and earlier does not properly honor CR0.TS and CR0.EM, which allows local x86 HVM guest OS users to read or modify FPU, MMX, or XMM register state information belonging to arbitrary tasks on the guest by modifying an instruction while the hypervisor is preparing to emulate it. **Reference: CVE-2016-7777**	http://xenbits.xen.org/xsa/advisory-190.html	O-XEN-XEN--201016/333

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10