Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Advanced Real Estate Script Project					
Advanced Real Estate Script					
XSS	03-01-2018	3.5	Online Ticket Booking has XSS via the admin/eventlist.php cast parameter. **CVE ID : CVE-2018-5078**	https://github.com/d4wner/Vulnerabilities-Report/blob/master/Advanced%20Real%20Estate%20Script.md	A-ADV-ADVAN-160118/1
XSS	03-01-2018	3.5	Online Ticket Booking has XSS via the admin/snacks_edit.php snacks_name parameter. **CVE ID : CVE-2018-5075**	https://github.com/d4wner/Vulnerabilities-Report/blob/master/Advanced%20Real%20Estate%20Script.md	A-ADV-ADVAN-160118/2
XSS	03-01-2018	3.5	Online Ticket Booking has XSS via the admin/manageownerlist.php contact parameter. **CVE ID : CVE-2018-5074**	https://github.com/d4wner/Vulnerabilities-Report/blob/master/Advanced%20Real%20Estate%20Script.md	A-ADV-ADVAN-160118/3
XSS	03-01-2018	3.5	Online Ticket Booking has XSS via the admin/sitesettings.php keyword parameter. **CVE ID : CVE-2018-5072**	https://github.com/d4wner/Vulnerabilities-Report/blob/master/Advanced%20Real%	A-ADV-ADVAN-160118/4

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				20Estate%20Script.md	
Advantech					
Webaccess					
NA	05-01-2018	5	An Improper Input Validation issue was discovered in Advantech WebAccess versions prior to 8.3. WebAccess allows some inputs that may cause the program to crash. **CVE ID : CVE-2017-16753**	NA	A-ADV-WEBAC-160118/5
NA	05-01-2018	5	An Untrusted Pointer Dereference issue was discovered in Advantech WebAccess versions prior to 8.3. There are multiple vulnerabilities that may allow an attacker to cause the program to use an invalid memory address, resulting in a program crash. **CVE ID : CVE-2017-16728**	NA	A-ADV-WEBAC-160118/6
Directory traversal	05-01-2018	5	A Path Traversal issue was discovered in WebAccess versions prior to 8.3. An attacker has access to files within the directory structure of the target device. **CVE ID : CVE-2017-16720**	NA	A-ADV-WEBAC-160118/7
Overflow	05-01-2018	7.5	A Stack-based Buffer Overflow issue was discovered in Advantech WebAccess versions prior to 8.3. There are multiple instances of a vulnerability that allows too much data to be written to a location on the stack. **CVE ID : CVE-2017-16724**	NA	A-ADV-WEBAC-160118/8
Sql	05-01-2018	7.5	A SQL Injection issue was discovered in WebAccess versions prior to 8.3. WebAccess does not properly sanitize its inputs for SQL commands. **CVE ID : CVE-2017-16716**	NA	A-ADV-WEBAC-160118/9
Awstats					
Awstats					
Execute Code	03-01-2018	7.5	Awstats version 7.6 and earlier is vulnerable to a path traversal flaw in	https://github.com/eldy/aws	A-AWS-AWSTA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory traversal			the handling of the "config" and "migrate" parameters resulting in unauthenticated remote code execution. **CVE ID : CVE-2017-1000501**	tats/commit/cf219843a74c951bf5986f3a7fffa3dcf99c3899	160118/10
BRO					
BRO					
DoS	02-01-2018	7.5	Bro before Bro v2.5.2 is vulnerable to an out of bounds write in the ContentLine analyzer allowing remote attackers to cause a denial of service (crash) and possibly other exploitation. **CVE ID : CVE-2017-1000458**	NA	A-BRO-BRO-160118/11
Cmsmadesimple					
Cms Made Simple					
File Inclusion	02-01-2018	4.6	CMS Made Simple 2.1.6, 2.2, 2.2.1 are vulnerable to Smarty Template Injection in some core components, resulting in local file read before 2.2, and local file inclusion since 2.2.1 **CVE ID : CVE-2017-1000454**	https://www.cmsmadesimple.org/2017/07/Announcing-CMSMS-2.2.2-Hearts-Content	A-CMS-CMSM-160118/12
Execute Code	02-01-2018	7.5	CMS Made Simple version 2.1.6 and 2.2 are vulnerable to Smarty templating injection in some core modules, resulting in unauthenticated PHP code execution. **CVE ID : CVE-2017-1000453**	https://www.cmsmadesimple.org/2017/06/Announcing-CMSMS-2-2-1-Hearts-Desire/	A-CMS-CMSM-160118/13
Creolabs					
Gravity					
Execute Code Overflow	02-01-2018	7.5	Creolabs Gravity 1.0 contains a stack based buffer overflow in the operator_string_add function, resulting in remote code execution. **CVE ID : CVE-2017-1000437**	https://github.com/marcobambini/gravity/issues/186	A-CRE-GRAVI-160118/14
Embedthis					
Goahead Web Server					
DoS	03-01-2018	5	EmbedThis GoAhead Webserver	NA	A-EMB-

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow			versions 4.0.0 and earlier is vulnerable to an integer overflow in the HTTP listener resulting in denial of service. **CVE ID : CVE-2017-1000470**		GOAHE-160118/15
Fork-cms					
Fork Cms					
XSS	04-01-2018	3.5	Fork CMS 5.0.7 has XSS in /private/en/pages/edit via the title parameter. **CVE ID : CVE-2018-5215**	https://github.com/imsebao/404team/blob/master/forkcms.md	A-FOR-FORK - 160118/16
IBM					
Security Key Lifecycle Manager					
NA	04-01-2018	4	IBM Tivoli Key Lifecycle Manager 2.5, 2.6, and 2.7 discloses sensitive information in error messages that could aid an attacker in further attacks against the system. IBM X-Force ID: 134869. **CVE ID : CVE-2017-1727**	http://www.ibm.com/support/docview.wss?uid=swg2201 2012	A-IBM-SECUR-160118/17
XSS	04-01-2018	4.3	IBM Tivoli Key Lifecycle Manager 2.5, 2.6, and 2.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 133640. **CVE ID : CVE-2017-1673**	http://www.ibm.com/support/docview.wss?uid=swg2201 2015	A-IBM-SECUR-160118/18
Gain Information	04-01-2018	4.3	IBM Tivoli Key Lifecycle Manager 2.5, 2.6, and 2.7 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 133636.	http://www.ibm.com/support/docview.wss?uid=swg2199 7955	A-IBM-SECUR-160118/19

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2017-1669		
NA	04-01-2018	4.3	IBM Tivoli Key Lifecycle Manager 2.5, 2.6, and 2.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 133559. **CVE ID : CVE-2017-1665**	http://www.ibm.com/support/docview.wss?uid=swg2201 2023	A-IBM-SECUR-160118/20
NA	04-01-2018	4.3	IBM Tivoli Key Lifecycle Manager 2.5, 2.6, and 2.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 133557. **CVE ID : CVE-2017-1664**	http://www.ibm.com/support/docview.wss?uid=swg2201 2027	A-IBM-SECUR-160118/21
CSRF	04-01-2018	6.8	IBM Tivoli Key Lifecycle Manager 2.6 and 2.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 133639. **CVE ID : CVE-2017-1672**	http://www.ibm.com/support/docview.wss?uid=swg2201 2019	A-IBM-SECUR-160118/22
Websphere Mq					
NA	04-01-2018	3.6	IBM MQ Managed File Transfer Agent 8.0 and 9.0 sets insecure permissions on certain files it creates. A local attacker could exploit this vulnerability to modify or delete data contained in the files with an unknown impact. IBM X-Force ID: 134391. **CVE ID : CVE-2017-1699**	http://www.ibm.com/support/docview.wss?uid=swg2201 0340	A-IBM-WEBSP-160118/23
NA	02-01-2018	4	IBM WebSphere MQ 8.0 and 9.0 could allow an authenticated user with authority to send a specially crafted request that could cause a channel process to cease processing further requests. IBM X-Force ID: 131547. **CVE ID : CVE-2017-1557**	http://www.ibm.com/support/docview.wss?uid=swg2200 4378	A-IBM-WEBSP-160118/24

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Imagemagick					
Imagemagick					
NA	01-01-2018	4.3	In ImageMagick 7.0.7-17 Q16, there is a Memory Leak in ReadPWPImage in coders/pwp.c. **CVE ID : CVE-2017-18008**	https://github.com/ImageMagick/ImageMagick/issues/921	A-IMA-IMAGE-160118/25
DoS	02-01-2018	4.3	ImageMagick 7.0.7-1 and older version are vulnerable to null pointer dereference in the MagickCore component and might lead to denial of service **CVE ID : CVE-2017-1000445**	https://github.com/ImageMagick/ImageMagick/issues/775	A-IMA-IMAGE-160118/26
NA	05-01-2018	4.3	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadRLAImage in coders/rla.c. **CVE ID : CVE-2018-5247**	https://github.com/ImageMagick/ImageMagick/issues/928	A-IMA-IMAGE-160118/27
NA	05-01-2018	4.3	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadPATTERNImage in coders/pattern.c. **CVE ID : CVE-2018-5246**	https://github.com/ImageMagick/ImageMagick/issues/929	A-IMA-IMAGE-160118/28
NA	05-01-2018	4.3	In ImageMagick 7.0.7-12 Q16, there are memory leaks in MontageImageCommand in MagickWand/montage.c. **CVE ID : CVE-2017-18022**	https://github.com/ImageMagick/ImageMagick/issues/904	A-IMA-IMAGE-160118/29
Overflow	05-01-2018	6.8	In ImageMagick 7.0.7-17 Q16, there is a heap-based buffer over-read in coders/sixel.c in the ReadSIXELImage function, related to the sixel_decode function. **CVE ID : CVE-2018-5248**	https://github.com/ImageMagick/ImageMagick/issues/927	A-IMA-IMAGE-160118/30
DoS	03-01-2018	7.1	ImageMagick 7.0.7-12 Q16, a CPU exhaustion vulnerability was found in the function ReadDDSInfo in coders/dds.c, which allows attackers to cause a denial of service. **CVE ID : CVE-2017-1000476**	NA	A-IMA-IMAGE-160118/31

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Invoiceninja					
Invoice Ninja					
Execute Code XSS	02-01-2018	3.5	Invoice Ninja version 3.8.1 is vulnerable to stored cross-site scripting vulnerability, within the invoice creation page, which can result in disruption of service and execution of javascript code. **CVE ID : CVE-2017-1000466**	https://github.com/invoiceninja/invoiceninja/issues/1727	A-INV-INVOI-160118/32
K7computing					
Antivirus					
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x8300211C. **CVE ID : CVE-2018-5088**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x8300211C	A-K7C-ANTIV-160118/33
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x83002100. **CVE ID : CVE-2018-5087**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x83002100	A-K7C-ANTIV-160118/34
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x8300215F. **CVE ID : CVE-2018-5086**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x8300215F	A-K7C-ANTIV-160118/35
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x83002124. **CVE ID : CVE-2018-5085**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x83002124	A-K7C-ANTIV-160118/36

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x8300212C. **CVE ID : CVE-2018-5084**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x8300212C	A-K7C-ANTIV-160118/37
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x8300215B. **CVE ID : CVE-2018-5083**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x8300215B	A-K7C-ANTIV-160118/38
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x83002128. **CVE ID : CVE-2018-5082**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x83002128	A-K7C-ANTIV-160118/39
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x830020F0. **CVE ID : CVE-2018-5081**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x830020F0	A-K7C-ANTIV-160118/40
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x830020FC. **CVE ID : CVE-2018-5080**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x830020FC	A-K7C-ANTIV-160118/41
DoS	03-01-2018	6.1	In K7 AntiVirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/0x83002130	A-K7C-ANTIV-160118/42

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			values from IOCtl 0x83002130. **CVE ID : CVE-2018-5079**		
DoS	04-01-2018	6.1	In K7 Antivirus 15.1.0306, the driver file (K7Sentry.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x95002610. **CVE ID : CVE-2018-5220**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/1_95002610	A-K7C-ANTIV-160118/43
DoS	04-01-2018	6.1	In K7 Antivirus 15.1.0306, the driver file (K7FWHlpr.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x83002168. **CVE ID : CVE-2018-5219**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/1_83002168	A-K7C-ANTIV-160118/44
DoS	04-01-2018	6.1	In K7 Antivirus 15.1.0306, the driver file (K7Sentry.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x950025b0. **CVE ID : CVE-2018-5218**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/1_950025b0	A-K7C-ANTIV-160118/45
DoS	04-01-2018	6.1	In K7 Antivirus 15.1.0306, the driver file (K7Sentry.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x95002578. **CVE ID : CVE-2018-5217**	https://github.com/rubyfly/K7AntiVirus_POC/tree/master/1_95002578	A-K7C-ANTIV-160118/46
Libtiff					
Libtiff					
NA	01-01-2018	4.3	In LibTIFF 4.0.9, there is a Null-Pointer Dereference in the tif_print.c TIFF Print Directory function, as demonstrated by a tiffinfo crash. **CVE ID : CVE-2017-18013**	https://gitlab.com/libtiff/libtiff/commit/c6f41df7b581402dfba3c19a1e3df4454c551a01	A-LIB-LIBTI-160118/47

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Marked Project					
Marked					
XSS	02-01-2018	4.3	marked version 0.3.6 and earlier is vulnerable to an XSS attack in the data: URI parser. **CVE ID : CVE-2017-1000427**	https://snyk.io/vuln/npm:marked:20170112	A-MAR-MARKE-160118/48
Mautic					
Mautic					
Directory traversal	03-01-2018	4	Mautic versions 1.0.0 - 2.11.0 are vulnerable to allowing any authorized Mautic user session (must be logged into Mautic) to use the Filemanager to download any file from the server that the web user has access to. **CVE ID : CVE-2017-1000490**	https://github.com/mautic/mautic/releases/tag/2.12.0	A-MAU-MAUTI-160118/49
XSS	03-01-2018	4.3	Mautic version 2.1.0 - 2.11.0 is vulnerable to an inline JS XSS attack when using Mautic forms on a Mautic landing page using GET parameters to pre-populate the form. **CVE ID : CVE-2017-1000488**	https://github.com/mautic/mautic/releases/tag/2.12.0	A-MAU-MAUTI-160118/50
NA	03-01-2018	6.8	Mautic versions 2.0.0 - 2.11.0 with a SSO plugin installed could allow a disabled user to still login using email address **CVE ID : CVE-2017-1000489**	https://github.com/mautic/mautic/releases/tag/2.12.0	A-MAU-MAUTI-160118/51
Microsoft					
Chakracore;Edge					
Gain Information	04-01-2018	4.3	Microsoft Edge in Microsoft Windows 10 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE ID : CVE-2018-0767 and CVE ID : CVE-2018-0780. **CVE ID : CVE-2018-0800**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2018-0800	A-MIC-CHAKR-160118/52

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Edge					
NA	04-01-2018	5.8	Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to access information from one domain and inject it into another domain, due to how Microsoft Edge enforces cross-domain policies, aka "Microsoft Edge Elevation of Privilege Vulnerability". **CVE ID : CVE-2018-0803**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2018-0803	A-MIC-EDGE-160118/53
Execute Code Overflow Memory Corruption	04-01-2018	7.6	Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0778. **CVE ID : CVE-2018-0781**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0781	A-MIC-EDGE-160118/54
Execute Code Overflow Memory Corruption	04-01-2018	7.6	Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0781. **CVE ID : CVE-2018-0778**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0778	A-MIC-EDGE-160118/55
Execute Code Overflow Memory	04-01-2018	7.6	Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the	https://portal.msrc.microsoft.com/en-	A-MIC-EDGE-160118/56

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Corruption			scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0778, and CVE-2018-0781. **CVE ID : CVE-2018-0777**	US/security-guidance/advisory/CVE-2018-0777	
Execute Code Overflow Memory Corruption	04-01-2018	7.6	Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781. **CVE ID : CVE-2018-0776**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0776	A-MIC-EDGE-160118/57
Execute Code Overflow Memory Corruption	04-01-2018	7.6	Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781. **CVE ID : CVE-2018-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0774	A-MIC-EDGE-160118/58
Opencv					
Opencv					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow	01-01-2018	5	In OpenCV 3.3.1, a heap-based buffer over-read exists in the function cv::HdrDecoder::checkSignature in modules/imgcodecs/src/grfmt_hdr.cpp. **CVE ID : CVE-2017-18009**	https://github.com/opencv/opencv/issues/10479	A-OPE-OPENC-160118/59
Openhacker Project					
Openhacker					
Execute Code Sql	02-01-2018	7.5	Eleix Openhacker version 0.1.47 is vulnerable to an SQL injection in the account registration and login component resulting in information disclosure and remote code execution **CVE ID : CVE-2017-1000444**	https://github.com/Eleix/openhacker/commit/9da5c237ba5e2311f01edc83389bc5aaf0a9885c	A-OPE-OPENH-160118/60
Passbolt					
Passbolt Api					
XSS	02-01-2018	3.5	Passbolt API version 1.6.4 and older are vulnerable to a XSS in the url field on the password workspace **CVE ID : CVE-2017-1000442**	https://www.passbolt.com/release/notes#September	A-PAS-PASSB-160118/61
Phpbb					
Phpbb					
NA	02-01-2018	5	phpBB version 3.2.0 is vulnerable to SSRF in the Remote Avatar function resulting allowing an attacker to perform port scanning, requesting internal content and potentially attacking such internal services via the web application. **CVE ID : CVE-2017-1000419**	https://www.phpbb.com/community/viewtopic.php?f=14&p=14782136	A-PHP-PHPBB-160118/62
Radiantcms					
Radiant Cms					
XSS	04-01-2018	3.5	Radiant CMS 1.1.4 has XSS via crafted Markdown input in the part_body_content parameter to an admin/pages/*/edit resource.	https://github.com/imsebao/404team/blob/mas	A-RAD-RADIA-160118/63

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-5216	ter/radiantcms.md	
Shiba Project					
Shiba					
Execute Code XSS	02-01-2018	4.3	Shiba markdown live preview app version 1.1.0 is vulnerable to XSS which leads to code execution due to enabled node integration. **CVE ID : CVE-2017-1000491**	https://github.com/rhysd/Shiba/commit/e8a65b0f81eb04903eedd29500d7e1bedf249eab	A-SHI-SHIBA-160118/64
Simple Download Monitor Project					
Simple Download Monitor					
XSS	04-01-2018	3.5	The Simple Download Monitor plugin before 3.5.4 for WordPress has XSS via the sdm_upload (aka Downloadable File) parameter in an edit action to wp-admin/post.php. **CVE ID : CVE-2018-5213**	NA	A-SIM-SIMPL-160118/65
XSS	04-01-2018	3.5	The Simple Download Monitor plugin before 3.5.4 for WordPress has XSS via the sdm_upload_thumbnail (aka File Thumbnail) parameter in an edit action to wp-admin/post.php. **CVE ID : CVE-2018-5212**	NA	A-SIM-SIMPL-160118/66
Structured-data					
Structured Data Linter					
Directory traversal	02-01-2018	5	Structured Data Linter versions 2.4.1 and older are vulnerable to a directory traversal attack in the URL input field resulting in the possibility of disclosing information about the remote host. **CVE ID : CVE-2017-1000448**	https://github.com/structured-data/linter/issues/41	A-STR-STRUC-160118/67
Syncthing					
Syncthing					
NA	02-01-2018	6.4	Syncthing version 0.14.33 and older is vulnerable to symlink traversal resulting	https://github.com/sync	A-SYN-SYNCT-

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in arbitrary file overwrite **CVE ID : CVE-2017-1000420**	thing/syncthing/issues/4286	160118/68
Z-url Preview Project					
Z-url Preview					
XSS	01-01-2018	4.3	The Z-URL Preview plugin 1.6.1 for WordPress has XSS via the class.zlinkpreview.php url parameter. **CVE ID : CVE-2017-18012**	NA	A-Z-U-Z-URL-160118/69
Hardware					
ARM;Intel					
Cortex-a/Atom C;Atom E;Atom X3;Atom Z;Celeron J;Celeron N;Core I3;Core I5;Core I7;Core M;Core M3;Core M5;Core M7;Pentium J;Pentium N;Xeon;Xeon Bronze;Xeon E3					
Gain Information	04-01-2018	4.7	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache. **CVE ID : CVE-2017-5754**	https://www.synology.com/support/security/Synology_SA_18_01	H-ARM-CORTE-160118/70
Gain Information	04-01-2018	4.7	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. **CVE ID : CVE-2017-5753**	https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html	H-ARM-CORTE-160118/71
Gain Information	04-01-2018	4.7	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. **CVE ID : CVE-2017-5715**	https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html	H-ARM-CORTE-160118/72
OPERATING SYSTEM(OS)					
Microsoft					
Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 1709;Windows Server 2008;Windows Server 2012;Windows Server 2016					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NA	04-01-2018	4.6	The Microsoft Server Message Block (SMB) Server in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way SMB Server handles specially crafted files, aka "Windows Elevation of Privilege Vulnerability". **CVE ID : CVE-2018-0749**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0749	O-MIC-WINDO-160118/73
NA	04-01-2018	4.6	The Windows kernel in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way memory addresses are handled, aka "Windows Elevation of Privilege Vulnerability". **CVE ID : CVE-2018-0748**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0748	O-MIC-WINDO-160118/74
NA	04-01-2018	3.6	The Windows Kernel API in Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way the Kernel API enforces permissions, aka "Windows Elevation of Privilege Vulnerability". This CVE ID is unique from CVE ID : CVE-2018-0752. **CVE ID : CVE-2018-0751**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0751	O-MIC-WINDO-160118/75
NA	04-01-2018	4.4	The Windows kernel in Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703	https://portal.msrc.microsoft.com/e	O-MIC-WINDO-160118/76

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka "Windows Elevation of Privilege Vulnerability". **CVE ID : CVE-2018-0744**	n-US/security-guidance/advisory/CVE-2018-0744	
NA	04-01-2018	4.6	The Windows Kernel API in Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way the Kernel API enforces permissions, aka "Windows Elevation of Privilege Vulnerability". This CVE ID is unique from CVE ID : CVE-2018-0751. **CVE ID : CVE-2018-0752**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0752	O-MIC-WINDO-160118/77
DoS Overflow	04-01-2018	7.1	Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allow a denial of service vulnerability due to the way objects are handled in memory, aka "Windows IPSec Denial of Service Vulnerability". **CVE ID : CVE-2018-0753**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0753	O-MIC-WINDO-160118/78
Windows 10;Windows Server 1709					
NA	04-01-2018	4.4	Windows Subsystem for Linux in Windows 10 version 1703, Windows 10 version 1709, and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka "Windows Subsystem for Linux Elevation of Privilege Vulnerability". **CVE ID : CVE-2018-0743**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0743	O-MIC-WINDO-160118/79

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;