Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Application (A)					
Apache					
Hadoop *The Apache Hadoop software library is a framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models*					
Gain Information	02-Jan-16	4	The Data Protection extension in the VMware GUI in IBM Tivoli Storage Manager for Virtual Environments: Data Protection for VMware (aka Spectrum Protect for Virtual Environments) 7.1 before 7.1.4 and Tivoli Storage FlashCopy Manager for VMware (aka Spectrum Protect Snapshot) 4.1 before 4.1.4 allows remote authenticated users to restore arbitrary virtual machines and consequently obtain sensitive information by visiting the vSphere inventory. ***Reference: CVE-2015-7429***	http://www-01.ibm.com/support/docview.wss?uid=isg3T1022979	A-APA-HADOO-181215/
Not Available	02-Jan-16	4.6	The Hadoop connector 1.1.1, 2.4, 2.5, and 2.7.0-0 before 2.7.0-3 for IBM Spectrum Scale and General Parallel File System (GPFS) allows local users to read or write to arbitrary GPFS data via unspecified vectors. ***Reference: CVE-2015-7430***		A-APA-HADOO-181215/
Cisco					
Prime Infrastructure *The Cisco Prime Infrastructure is a network management tool that provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices*					
Cross Site Scripting	07-Jan-16	4.3	Cisco Prime Infrastructure does not properly restrict use of IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks and unspecified other attacks via a crafted web site, related to a "cross-frame scripting (XFS)" issue, aka Bug ID CSCux64856. ***Reference: CVE-2015-6434***	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160105-pi	A-CIS-PRIME-181215/
Unified Communications Manager *Cisco Unified Communications Manager (Unified CM) is the industry leader in enterprise call and session management platforms. It delivers people-centric user and administrative experiences while supporting the full range of collaboration services including video, voice, IM and presence, messaging, and mobility on Cisco as well as third-party devices*					
Execute Code;	07-Jan-16	4	SQL injection vulnerability in Cisco	http://tools.cisco.co	A-CIS-

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Sql Injection			Unified Communications Manager 11.0(0.98000.225) allows remote authenticated users to execute arbitrary SQL commands via a crafted URL, aka Bug ID CSCut66767. ***Reference: CVE-2015-6433***	m/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160105-cucm	UNIFI-181215/
Dx Library Project					
Dx Library *DX Library is a Python-based financial analytics library (in its early stages) which allows the modeling of rather complex derivatives instruments and portfolios.*					
Execute Code; Overflow	07-Jan-16	6.8	Buffer overflow in the CL_vsprintf function in Takumi Yamada DX Library before 3.16 allows remote attackers to execute arbitrary code via a crafted string. ***Reference: CVE-2016-1131***	http://homepage2.nifty.com/natupaji/DxLib/dxvulnerability.html	A-DX -DX LIB-181215/
Eucalyptus					
Eucalyptus *Eucalyptus is free and open-source computer software for building Amazon Web Software project, at Rice University and other institutions from 2003 to 2008.*					
Bypass	04-Jan-16	4.6	HP Helion Eucalyptus 4.1.x before 4.1.2 and HPE Helion Eucalyptus 4.2.x before 4.2.1 allow remote authenticated users to bypass intended access restrictions and modify arbitrary (1) access key credentials by leveraging knowledge of a key ID or (2) signing certificates by leveraging knowledge of a certificate ID. ***Reference: CVE-2014-5040***	https://www.eucalyptus.com/resources/security/advisories/esa-32	A-EUC-EUCAL-181215/
Bypass	05-Jan-16	4.6	HPE Helion Eucalyptus 3.4.0 through 4.2.0 allows remote authenticated users to bypass an intended AssumeRole permission requirement and assume an IAM role by leveraging a policy setting for a user's account. ***Reference: CVE-2015-6861***	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04926482	A-EUC-EUCAL-181215/
HP					
Insight Management *IM is the basis for the HP system management tools and is part of HP's unified infrastructure management strategy, as well as HP Insight Control.*					
Gain Information	05-Jan-16	4.3	HP Insight Control server provisioning before 7.5.0 RabbitMQ allows remote attackers to obtain sensitive information via unspecified vectors. ***Reference: CVE-2015-6858***	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04918653	A-HP-INSIG-181215/
Bypass; Gain Information	07-Jan-16	7.2	HPE UCMDB Browser before 4.02 allows remote attackers to obtain sensitive information or bypass intended access restrictions via	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=	A-HP-UCMDB-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			unspecified vectors. ***Reference: CVE-2015-6862***	emr_na-c04924053	
IBM					
B2b Advanced Communications; Multi-enterprise Integration Gateway *B2B Advanced Communications provides optimized and dynamic end-to-end information flows. Multi-Enterprise Integration Gateway V1.0 delivers the high availability communications architecture necessary to sustain the demands of a global real-time, response driven, value chain.*					
Gain Information	01-Jan-16	3.5	IBM Multi-Enterprise Integration Gateway 1.0 through 1.0.0.1 and B2B Advanced Communications 1.x before 1.0.0.4, when guest access is configured, allow remote authenticated users to obtain sensitive information by reading error messages in responses. ***Reference: CVE-2015-7445***	http://www-01.ibm.com/support/docview.wss?uid=swg21972480	A-IBM-B2BA-181215/
Change And Configuration Management Database; Maximo Asset Management Essentials; Maximo For Energy Optimization; Maximo For Government; Maximo For Life Sciences; Maximo For Nuclear Power; Maximo For Oil And Gas Maximo For Transportation; Maximo For Utilities; Smartcloud Control Desk; Tivoli Asset Management For It; Tivoli Service Request Manager *A configuration management database (CMDB) is a repository that acts as a data warehouse for information technology (IT) organizations. Maximo Asset Management Essentials is ideal for smaller organizations that require a subset of the extensive range of features. IBM Maximo Asset Management for Energy Optimization helps optimize energy efficiency and reduce risk with visual mapping of key energy and environmental metrics. IBM Tivoli Asset Management for IT software enables organizations to optimize software licenses and manage IT asset lifecycles in order to control cost. IBM Tivoli Service Request Manager wiki, a collaborative repository of technical information.*					
Bypass	03-Jan-16	5.5	IBM Maximo Asset Management 7.1 through 7.1.1.13, 7.5.0 before 7.5.0.8 IFIX005, and 7.6.0 before 7.6.0.2 IFIX002; Maximo Asset Management 7.5.0 before 7.5.0.8 IFIX005, 7.5.1, and 7.6.0 before 7.6.0.2 IFIX002 for SmartCloud Control Desk; and Maximo Asset Management 7.1 through 7.1.1.13 and 7.2 for Tivoli IT Asset Management for IT and certain other products allow remote authenticated users to bypass intended access restrictions and establish a login session by entering an expired password. ***Reference: CVE-2015-5017***	http://www-01.ibm.com/support/docview.wss?uid=swg21969052	A-IBM-CMDB-181215/
Connections *IBM Connections Suite provides IBM social solutions, including software, real-time social communications and content management capabilities.*					
Cross Site Scripting	03-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in IBM Connections 3.x before 3.0.1.1 CR3, 4.0 before CR4, 4.5 before CR5, and 5.0 before CR3	http://www-01.ibm.com/support/docview.wss?uid=swg21971439	A-IBM-CONNE-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL, a different vulnerability than CVE-2015-5036. ***Reference: CVE-2015-5035***		
Cross Site Scripting	03-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in IBM Connections 3.x before 3.0.1.1 CR3, 4.0 before CR4, 4.5 before CR5, and 5.0 before CR3 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL, a different vulnerability than CVE-2015-5035. ***Reference: CVE-2015-5036***		A-IBM-CONNE-181215/
Cross Site Scripting	03-Jan-16	6.8	Cross-site request forgery (CSRF) vulnerability in IBM Connections 3.x before 3.0.1.1 CR3, 4.0 before CR4, 4.5 before CR5, and 5.0 before CR3 allows remote authenticated users to hijack the authentication of arbitrary users for requests that insert XSS sequences. ***Reference: CVE-2015-5037***		A-IBM-CONNE-181215/
Denial of Service	03-Jan-16	7.8	IBM Connections 3.x before 3.0.1.1 CR3, 4.0 before CR4, 4.5 before CR5, and 5.0 before CR3 does not properly detect recursion during XML entity expansion, which allows remote attackers to cause a denial of service (CPU consumption and application crash) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564. ***Reference: CVE-2015-5038***		A-IBM-CONNE-181215/
Curam Social Program Management *Curam Social Program Management Platform delivers prebuilt social program components, business processes, toolsets and interfaces*					
Cross Site Scripting	02-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in IBM Curam Social Program Management 6.1 before 6.1.1.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. ***Reference: CVE-2015-7402***	http://www-01.ibm.com/support/docview.wss?uid=swg21970661	A-IBM-CURAM-181215/
Execute Code; Sql Injection	03-Jan-16	6.5	SQL injection vulnerability in IBM Curam Social Program Management 6.1 before 6.1.1 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. ***Reference: CVE-2015-5023***		A-IBM-CURAM-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
General Parallel File System; Spectrum Scale *The General Parallel File System (GPFS) is a high-performance clustered file system developed by IBM.* *IBM Spectrum Scale provides simplified data management and integrated information lifecycle tools capable of managing petabytes of data and billions of files.*					
Denial of Service	02-Jan-16	2.1	IBM Spectrum Scale 4.1.1.x before 4.1.1.3 and General Parallel File System (GPFS) 3.5.x before 3.5.0.29 and 4.1.x through 4.1.0.8 on AIX allow local users to cause a denial of service (incorrect pointer dereference and node crash) via unspecified vectors. ***Reference: CVE-2015-7403***	http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005452	A-IBM-GENER-181215/
I Access *IBM i Access is to bring the power of the Power Systems servers to the desktop, browser.*					
Denial of Service	02-Jan-16	2.1	AFP Workbench Viewer in IBM i Access 7.1 on Windows allows remote attackers to cause a denial of service (viewer crash) via a crafted workbench file. ***Reference: CVE-2015-7416***	http://www-01.ibm.com/support/docview.wss?uid=nas8N1020995	A-IBM-IACCE-181215/
Denial of Service; Overflow	02-Jan-16	2.1	Buffer overflow in IBM i Access 7.1 on Windows allows local users to cause a denial of service (application crash) via unspecified vectors. ***Reference: CVE-2015-7422***		A-IBM-IACC-181215/
Overflow;Gain Privileges	02-Jan-16	7.2	Buffer overflow in IBM i Access 7.1 on Windows allows local users to gain privileges via unspecified vectors. ***Reference: CVE-2015-2023***	http://www-01.ibm.com/support/docview.wss?uid=nas8N1020996	A-IBM-IACC-181215/
Infosphere Biginsights *IBM InfoSphere BigInsights brings the power of Hadoop to the enterprise. Apache `Hadoop is the open source software framework, used to reliably manage large volumes of structured and unstructured data.*					
Not Available	02-Jan-16	4	The Big SQL component in IBM InfoSphere BigInsights 3.0, 3.0.0.1, 3.0.0.2, and 4.0 allows remote authenticated users to bypass intended access restrictions and truncate arbitrary tables via unspecified vectors. ***Reference: CVE-2015-5020***	http://www-01.ibm.com/support/docview.wss?uid=swg21967923	A-IBM-INFOS-181215/
Installation Manager; Packaging Utility *IBM Installation Manager is an application that makes it easier to download, install, and update code for IBM software products.* *IBM Packaging Utility software to set up a repository for IBM Installation Manager and to copy product packages to the repository.*					
Gain Privileges	02-Jan-16	6.2	consoleinst.sh in IBM Installation Manager before 1.7.4.4 and 1.8.x before 1.8.4 and Packaging Utility before 1.7.4.4 and 1.8.x before 1.8.4 allows local users to gain privileges via a Trojan horse program that is located in /tmp with a name based on	http://www-01.ibm.com/support/docview.wss?uid=swg21971295	A-IBM-INSTA-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			a predicted PID value. ***Reference: CVE-2015-7442***		
Mashups Center *IBM Mashup Center is an end-to-end enterprise mashup platform that enables the rapid creation, sharing, and discovery of reusable application building.*					
Denial of Service	02-Jan-16	6.8	The Lotus Mashups component in IBM Mashup Center 3.0.0.1 allows remote authenticated users to cause a denial of service (CPU consumption) via an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. ***Reference: CVE-2015-7400***	http://www-01.ibm.com/support/docview.wss?uid=swg21970392	A-IBM-MASHU-181215/
Cross Site Scripting; Cross-site Request Forgery	02-Jan-16	6.8	Cross-site request forgery (CSRF) vulnerability in Lotus Mashups in IBM Mashup Center 3.0.0.1 allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences. ***Reference: CVE-2015-7407***	http://www-01.ibm.com/support/docview.wss?uid=swg21970299	A-IBM-MASHU-181215/
Maximo Asset Management; Maximo Asset Management Essentials; Maximo For Government; Maximo For Life Sciences; Maximo For Nuclear Power; Maximo For Oil And Gas; Maximo For Transportation; Maximo For Utilities; Smartcloud Control Desk *Maximo Asset Management Essentials is ideal for smaller organizations that require a subset of the extensive range of features.* *IBM Maximo Asset Management for Energy Optimization helps optimize energy efficiency and reduce risk with visual mapping of key energy and environmental metrics.*					
Cross Site Scripting	02-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in IBM Maximo Asset Management 7.5 before 7.5.0.9 IF2 and 7.6 before 7.6.0.3 FP3 and Maximo Asset Management 7.5 before 7.5.0.9 IF2, 7.5.1, and 7.6 before 7.6.0.3 FP3 for SmartCloud Control Desk allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. ***Reference: CVE-2015-7451***	http://www-01.ibm.com/support/docview.wss?uid=swg21970797	A-IBM-MAXIM-181215/
Gain Information	02-Jan-16	4	IBM Maximo Asset Management 7.5 before 7.5.0.9 FP9 and 7.6 before 7.6.0.3 FP3 and Maximo Asset Management 7.5 before 7.5.0.9 FP9, 7.5.1, and 7.6 before 7.6.0.3 FP3 for SmartCloud Control Desk allow remote authenticated users to obtain sensitive information via the REST API. ***Reference: CVE-2015-7452***		A-IBM-MAXIM-181215/
Bypass	03-Jan-16	4	IBM Maximo Asset Management 7.5 before 7.5.0.8 IF6 and 7.6 before		A-IBM-MAXIM-

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			7.6.0.2 IF1 and Maximo Asset Management 7.5 before 7.5.0.8 IF6, 7.5.1, and 7.6 before 7.6.0.2 IF1 for SmartCloud Control Desk allow remote authenticated users to bypass intended access restrictions on query results via unspecified vectors. ***Reference: CVE-2015-5051***		181215/
Bypass; Gain Information	02-Jan-16	5.5	The Scheduler in IBM Maximo Asset Management 7.5 before 7.5.0.8 IF6 and 7.6 before 7.6.0.1 FP1 and Maximo Asset Management 7.5 before 7.5.0.8 IF6, 7.5.1, and 7.6 before 7.6.0.1 FP1 for SmartCloud Control Desk allows remote authenticated users to bypass intended access restrictions, and obtain sensitive information or modify data, via unspecified vectors. *Reference: CVE-2015-7396*		A-IBM-MAXIM-181215/
Mq Appliance M2000 *MQ Appliance M2000 provides the application connectivity performance of IBM MQ software in a physical messaging appliance.*					
Bypass	02-Jan-16	1.9	The queue manager on IBM MQ M2000 appliances before 8.0.0.4 allows local users to bypass an intended password requirement and read private keys by leveraging the existence of a stash file. ***Reference: CVE-2015-1985***	http://www-01.ibm.com/support/docview.wss?uid=swg21971445	A-IBM-MQAPP-181215/
Gain Information	01-Jan-16	5	Unspecified vulnerability in GSKit on IBM MQ M2000 appliances before 8.0.0.4 allows remote attackers to obtain sensitive information via unknown vectors, a different vulnerability than CVE-2015-7421. ***Reference: CVE-2015-7420***	http://www-01.ibm.com/support/docview.wss?uid=swg21971500	A-IBM-MQAPP-181215/
Openpages Grc Platform *OpenPages GRC Platform is an integrated governance, risk and compliance platform that enables companies to manage risk and regulatory challenges*					
Execute Code; Sql Injection	01-Jan-16	6.5	SQL injection vulnerability in the API in IBM OpenPages GRC Platform 7.0 before 7.0.0.4 IF3 and 7.1 before 7.1.0.1 IF6 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. ***Reference: CVE-2015-5049***	http://www-01.ibm.com/support/docview.wss?uid=swg21970590	A-IBM-OPENP-181215/
Qradar Security Information And Event Manager *IBM Security Qradar SIEM consolidates log source event data from thousands of devices endpoints and applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives.*					

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Cross Site Scripting	01-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in IBM Security QRadar SIEM 7.2.x before 7.2.6 allows remote authenticated users to inject arbitrary web script or HTML via an unspecified field. ***Reference: CVE-2015-7409***	http://www-01.ibm.com/support/docview.wss?uid=swg21973175	A-IBM-QRADA-181215/
Directory Traversal	02-Jan-16	4	Directory traversal vulnerability in IBM Security QRadar SIEM 7.2.x before 7.2.5 Patch 6 allows remote authenticated users to read arbitrary files via a crafted URL. ***Reference: CVE-2015-2007***	http://www-01.ibm.com/support/docview.wss?uid=swg21967647	A-IBM-QRADA-181215/
Rational Clearquest *Rational ClearQuest is an enterprise level workflow automation tool from the Rational Software division of IBM. Commonly, ClearQuest is configured as a bug tracking system, but it can be configured to act as a CRM tool or to track a complex manufacturing process.*					
Gain Information	02-Jan-16	3.6	IBM Rational ClearQuest 7.1.x and 8.0.0.x before 8.0.0.17 and 8.0.1.x before 8.0.1.10 allows local users to spoof database servers and discover credentials via unspecified vectors. ***Reference: CVE-2015-4996***	http://www-01.ibm.com/support/docview.wss?uid=swg21972331	A-IBM-RATIO-181215/
Rational Collaborative Lifecycle Management; Rational Doors Next Generation; Rational Engineering Lifecycle Manager; Rational Quality Manager; Rational Requirements Composer; Rational Rhapsody Design Manager; Rational Software Architect Design Manager; Rational Team Concert *The IBM CLM suite integrates with other tools which provide further automation or support for various steps in the software development lifecycle. IBM Rational DOORS Next Generation has a full range of benefits to help you collaborate more effectively, so you can work faster, trace changes. IBM Rational Engineering Lifecycle Manager visualizes, analyzes and organizes engineering lifecycle data and data relationships. IBM Rational Software Architect Design Manager based on jazz platform enables collaborative design management of models authored by Rational Software Rational Team Concert is a software development team collaboration tool developed by the Rational Software brand of IBM, who first released it in 2008. The software is available in both client versions and a Web version.*					
Bypass	03-Jan-16	2.1	Rational LifeCycle Project Administration in Jazz Team Server in IBM Rational Collaborative Lifecycle Management (CLM) 3.x and 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Quality Manager (RQM) 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Team Concert (RTC) 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Requirements Composer (RRC) 3.x before 3.0.1.6 IF7 and 4.x before 4.0.7 IF9; Rational DOORS Next Generation (RDNG) 4.x before	http://www-01.ibm.com/support/docview.wss?uid=swg21973404	A-IBM-RATIO-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Engineering Lifecycle Manager (RELM) 4.x through 4.0.7, 5.x through 5.0.2, and 6.x before 6.0.1; Rational Rhapsody Design Manager (DM) 4.x through 4.0.7, 5.x through 5.0.2, and 6.x before 6.0.1; and Rational Software Architect Design Manager (DM) 4.x through 4.0.7, 5.x through 5.0.2, and 6.x before 6.0.1 allows local users to bypass intended access restrictions via unspecified vectors. ***Reference: CVE-2015-4946***		
Gain Information	03-Jan-16	2.7	Jazz Team Server in Jazz Foundation in IBM Rational Collaborative Lifecycle Management (CLM) 3.x and 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Quality Manager (RQM) 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Team Concert (RTC) 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Requirements Composer (RRC) 3.x before 3.0.1.6 IF7 and 4.x before 4.0.7 IF9; Rational DOORS Next Generation (RDNG) 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF9, and 6.x before 6.0.1; Rational Engineering Lifecycle Manager (RELM) 4.x through 4.0.7, 5.x through 5.0.2, and 6.x before 6.0.1; Rational Rhapsody Design Manager (DM) 4.x through 4.0.7, 5.x through 5.0.2, and 6.x before 6.0.1; and Rational Software Architect Design Manager (DM) 4.x through 4.0.7, 5.x through 5.0.2, and 6.x before 6.0.1 uses weak permissions for unspecified project areas, which allows remote authenticated users to obtain sensitive information via unknown vectors. ***Reference: CVE-2015-4962***	http://www-01.ibm.com/support/docview.wss?uid=swg21973405	A-IBM-RATIO-181215/
Denial of Service	02-Jan-16	3.3	Unspecified vulnerability in Jazz Team Server in Jazz Foundation in IBM Rational Collaborative Lifecycle Management (CLM) 3.x and 4.x before 4.0.7 IF8 and 5.x before 5.0.2 IF10; Rational Quality Manager (RQM) 2.x	http://www-01.ibm.com/support/docview.wss?uid=swg21971164	A-IBM-RATIO-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			and 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF8, and 5.x before 5.0.2 IF10; Rational Team Concert (RTC) 2.x and 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF8, and 5.x before 5.0.2 IF10; Rational Requirements Composer (RRC) 2.x and 3.x before 3.0.1.6 IF7 and 4.0 through 4.0.7; Rational DOORS Next Generation (RDNG) 4.x before 4.0.7 IF8 and 5.x before 5.0.2 IF10; Rational Engineering Lifecycle Manager (RELM) 1.0 through 1.0.0.1, 4.0.3 through 4.0.7, and 5.0 through 5.0.2; Rational Rhapsody Design Manager (DM) 3.0 through 3.0.1, 4.0 through 4.0.7, 5.0 through 5.0.2, and 6.0; and Rational Software Architect Design Manager (DM) 3.0 through 3.0.1, 4.0 through 4.0.7, and 5.0 through 5.0.2 allows remote attackers to cause a denial of service via unknown vectors. ***Reference: CVE-2015-1971***		
Not Available	02-Jan-16	3.5	Jazz Team Server in Jazz Foundation in IBM Rational Collaborative Lifecycle Management (CLM) 3.x and 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF11, and 6.x before 6.0.0 IF4; Rational Quality Manager (RQM) 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF11, and 6.0 before 6.0.0 IF4; Rational Team Concert (RTC) 3.x before 3.0.1.6 IF7, 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF11, and 6.0 before 6.0.0 IF4; Rational Requirements Composer (RRC) 3.x before 3.0.1.6 IF7 and 4.x before 4.0.7 IF9; Rational DOORS Next Generation (RDNG) 4.x before 4.0.7 IF9, 5.x before 5.0.2 IF11, and 6.0 before 6.0.0 IF4; Rational Engineering Lifecycle Manager (RELM) 4.0.3 through 4.0.7, 5.0 through 5.0.2, and 6.0.0; Rational Rhapsody Design Manager (DM) 4.0 through 4.0.7, 5.0 through 5.0.2, and 6.0.0; and Rational Software Architect Design Manager (DM) 4.0 through 4.0.7, 5.0 through 5.0.2, and 6.0.0 allows remote authenticated users to conduct clickjacking attacks via a crafted web site. ***Reference: CVE-2015-1928***	http://www-01.ibm.com/support/docview.wss?uid=swg21973200	A-IBM-RATIO-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Spectrum Protect For Virtual Environments; Spectrum Protect Snapshot *IBM Spectrum Protect for Virtual Environments (formerly IBM Tivoli Storage Manager for Virtual Environments) protects VMware and Microsoft Hyper-V virtual machines. It enables you to safeguard the massive amounts of information that virtual machines generate.* *Spectrum Protect Snapshot, formerly Tivoli Storage FlashCopy Manager, delivers high levels of protection for key applications and databases using advanced integrated application snapshot backup and restore capabilities.*					
Execute Code	02-Jan-16	10	The Data Protection extension in the VMware GUI in IBM Tivoli Storage Manager for Virtual Environments: Data Protection for VMware (aka Spectrum Protect for Virtual Environments) 7.1 before 7.1.3.0 and Tivoli Storage FlashCopy Manager for VMware (aka Spectrum Protect Snapshot) 4.1 before 4.1.3.0 allows remote attackers to execute arbitrary OS commands via unspecified vectors. ***Reference: CVE-2015-7426***	http://www-01.ibm.com/support/docview.wss?uid=swg21971484	A-IBM-SPECT-181215/
Spectrum Scale *Spectrum Scale provides simplified data management and integrated information lifecycle tools capable of managing petabytes of data and billions of files*					
Gain Information	01-Jan-16	4	IBM Spectrum Scale 4.1.1 before 4.1.1.4, and 4.2.0.0, allows remote authenticated users to discover object-storage admin passwords via unspecified vectors. ***Reference: CVE-2015-7456***	http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005476	A-IBM-SPECT-181215/
Sterling B2b Integrator *IBM Sterling B2B Integrator enables the security-rich integration of complex B2B processes with diverse partner communities.*					
Gain Information	02-Jan-16	1.9	IBM Sterling B2B Integrator 5.2 allows local users to obtain sensitive cleartext web-services information by leveraging database access. ***Reference: CVE-2015-7438***	http://www-01.ibm.com/support/docview.wss?uid=swg21972676	A-IBM-STERL-181215/
Gain Information	02-Jan-16	2.1	Queue Watcher in IBM Sterling B2B Integrator 5.2 allows local users to obtain sensitive information via unspecified vectors. ***Reference: CVE-2015-7437***		A-IBM-STERL-181215/
Cross Site Scripting	02-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Queue Watcher in IBM Sterling B2B Integrator 5.2 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. ***Reference: CVE-2015-7431***		A-IBM-STERL-181215/
Gain Information	01-Jan-16	5.8	The Health Check tool in IBM Sterling B2B Integrator 5.2 does not properly use cookies in conjunction with HTTPS sessions, which allows man-		A-IBM-STERL-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			in-the-middle attackers to obtain sensitive information or modify data via unspecified vectors. ***Reference: CVE-2015-7410***		
Tealeaf Customer Experience *Tealeaf a leading provider of digital customer experience management and customer behavior analysis solutions.*					
Gain Information	02-Jan-16	1.9	The portal in IBM Tealeaf Customer Experience before 8.7.1.8818, 8.8 before 8.8.0.9026, 9.0.0, 9.0.0A, 9.0.1 before 9.0.1.1083, 9.0.1A before 9.0.1.5073, 9.0.2 before 9.0.2.1095, and 9.0.2A before 9.0.2.5144 allows local users to discover credentials by leveraging privileges during an unspecified connection type. ***Reference: CVE-2015-4990***	http://www-01.ibm.com/support/docview.wss?uid=swg21969739	A-IBM-TEALE-181215/
Gain Information	02-Jan-16	5	The portal in IBM Tealeaf Customer Experience before 8.7.1.8814, 8.8 before 8.8.0.9026, 9.0.0, 9.0.0A, 9.0.1 before 9.0.1.1083, 9.0.1A before 9.0.1.5073, 9.0.2 before 9.0.2.1095, and 9.0.2A before 9.0.2.5144 allows remote attackers to read arbitrary charts by specifying an internal chart name. ***Reference: CVE-2015-4989***	http://www-01.ibm.com/support/docview.wss?uid=swg21968866	A-IBM-TEALE-181215/
Tivoli Common Reporting *Tivoli Common Reporting (TCR) is the Tivoli standard infrastructure for creating, viewing, and managing Tivoli product report.*					
Bypass	02-Jan-16	1.9	IBM Tivoli Common Reporting (TCR) 2.1 before IF14, 2.1.1 before IF22, 2.1.1.2 before IF9, 3.1.0.0 through 3.1.2 as used in Cognos Business Intelligence before 10.2 IF16, and 3.1.2.1 as used in Cognos Business Intelligence before 10.2.1.1 IF12 allows local users to bypass the Cognos Application Firewall (CAF) protection mechanism via leading whitespace in the BackURL field. ***Reference: CVE-2015-7435***	http://www-01.ibm.com/support/docview.wss?uid=swg21972799	A-IBM-TIVOL-181215/
Bypass	02-Jan-16	1.9	IBM Tivoli Common Reporting (TCR) 2.1 before IF14, 2.1.1 before IF22, 2.1.1.2 before IF9, 3.1.0.0 through 3.1.2 as used in Cognos Business Intelligence before 10.2 IF16, and 3.1.2.1 as used in Cognos Business Intelligence before 10.2.1.1 IF12 preserves user permissions across group-add and group-remove operations, which allows local users	http://www-01.ibm.com/support/docview.wss?uid=swg21972800	A-IBM-TIVOL-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			to bypass intended access restrictions in opportunistic circumstances by leveraging administrative changes to group membership. ***Reference: CVE-2015-7436***		
Execute Code	02-Jan-16	10	IBM Tivoli Common Reporting (TCR) 2.1 before IF14, 2.1.1 before IF22, 2.1.1.2 before IF9, 3.1.0.0 through 3.1.2 as used in Cognos Business Intelligence before 10.2 IF16, and 3.1.2.1 as used in Cognos Business Intelligence before 10.2.1.1 IF12 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the InvokerTransformer class in the Apache Commons Collections library. ***Reference: CVE-2015-7450***	http://www-01.ibm.com/support/docview.wss?uid=swg21972799	A-IBM-TIVOL-181215/
Tivoli Monitoring *IBM Tivoli Monitoring and Tivoli Composite Application Manager products help optimize IT infrastructure performance and availability.*					
Execute Code	03-Jan-16	8.5	The portal in IBM Tivoli Monitoring (ITM) 6.2.2 through FP9, 6.2.3 through FP5, and 6.3.0 before FP7 allows remote authenticated users to execute arbitrary commands by leveraging Take Action view authority and providing crafted input. ***Reference: CVE-2015-5003***	http://www-01.ibm.com/support/docview.wss?uid=swg21970361	A-IBM-TIVOL-181215/
Urbancode Deploy *UrbanCode Deploy is a tool for automating application deployments through your environments. It is designed to facilitate rapid feedback and continuous delivery in agile development while providing the audit trails, versioning and approvals needed in production.*					
Cross Site Scripting	01-Jan-16	3.5	Multiple cross-site scripting (XSS) vulnerabilities in IBM UrbanCode Deploy 6.0 before 6.0.1.12, 6.1 before 6.1.3.2, and 6.2 before 6.2.0.2 allow remote authenticated users to inject arbitrary web script or HTML via a crafted URL. ***Reference: CVE-2015-7415***	http://www-01.ibm.com/support/docview.wss?uid=swg21970811	A-IBM-URBAN-181215/
Websphere Mq Light *MQ Light for Bluemix is a cloud-based messaging service, built on the Advanced Message Queuing Protocol (AMQP)*					
Denial of Service	01-Jan-16	5	IBM WebSphere MQ Light 1.x before 1.0.2 mishandles abbreviated TLS handshakes, which allows remote attackers to cause a denial of service (MQXR service crash) via unspecified vectors. ***Reference: CVE-2015-4941***	http://www-01.ibm.com/support/docview.wss?uid=swg21972019	A-IBM-WEBSP-181215/
Denial of	01-Jan-16	5	IBM WebSphere MQ Light 1.x before	https://www-	A-IBM-

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Service			1.0.2 allows remote attackers to cause a denial of service (MQXR service crash) via a series of connect and disconnect actions. ***Reference: CVE-2015-4943***	01.ibm.com/support/docview.wss?uid=swg21972021	WEBSP-181215/
Ipswitch					
Whatsup Gold *WhatsUp Gold simplifies complete IT monitoring through network monitoring, application performance management, and server monitoring solutions.*					
Sql Injection	07-Jan-16	7.5	The DroneDeleteOldMeasurements implementation in Ipswitch WhatsUp Gold before 16.4 does not properly validate serialized XML objects, which allows remote attackers to conduct SQL injection attacks via a crafted SOAP request. ***Reference: CVE-2015-8261***	https://www.kb.cert.org/vuls/id/753264	A-IPS-WHATS-181215/
Mozilla					
Bugzilla *Bugzilla is a web-based general-purpose bugtracker and testing tool originally developed and used by the Mozilla project, and licensed under the Mozilla Public License.*					
Cross Site Scripting	03-Jan-16	2.6	Cross-site scripting (XSS) vulnerability in showdependencygraph.cgi in Bugzilla 2.x, 3.x, and 4.x before 4.2.16, 4.3.x and 4.4.x before 4.4.11, and 4.5.x and 5.0.x before 5.0.2, when a local dot configuration is used, allows remote attackers to inject arbitrary web script or HTML via a crafted bug summary. ***Reference: CVE-2015-8508***	https://bugzilla.mozilla.org/show_bug.cgi?id=1221518	A-MOZ-BUGZI-181215/
Gain Information	03-Jan-16	4.3	Template.pm in Bugzilla 2.x, 3.x, and 4.x before 4.2.16, 4.3.x and 4.4.x before 4.4.11, and 4.5.x and 5.0.x before 5.0.2 does not properly construct CSV files, which allows remote attackers to obtain sensitive information by leveraging a web browser that interprets CSV data as JavaScript code. ***Reference: CVE-2015-8509***		A-MOZ-BUGZI-181215/
Nodejs					
Node.js *Node.js is an open-source, cross-platform runtime environment for developing server-side web applications.*					
Denial of Service	02-Jan-16	5	Node.js 0.12.x before 0.12.9, 4.x before 4.2.3, and 5.x before 5.1.1 does not ensure the availability of a parser for each HTTP socket, which allows remote attackers to cause a denial of service (uncaughtException and service outage) via a pipelined HTTP	https://nodejs.org/en/blog/vulnerability/cve-2015-8027_cve-2015-6764/	A-NOD-NODE.-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			request. ***Reference: CVE-2015-8027***		
Pcre					
Perl Compatible Regular Expression Library *Perl-compatible regular expressions library used in projects such as PHP. Includes download, documentation and contact information.*					
Denial of Service; Overflow	02-Jan-16	7.5	The pcre_compile2 function in pcre_compile.c in PCRE 8.38 mishandles the /((?:F?+(?:^(?(R)a+\"){99}))(?J)(?'R'(?'R'<((?'RR'(?'R'\){97)?J)?J)(?'R'(?'R'\){99|(:(?|(?'R')(\k'R')|((?'R')))H'R'R)(H'R)))))/ pattern and related patterns with named subgroups, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror. ***Reference: CVE-2016-1283***	https://bugs.exim.org/show_bug.cgi?id=1767	A-PCR-PERL-181215/
Wireshark					
Wireshark *Wireshark is the network protocol analyzer. It lets you see what's happening on your network at a microscopic level.*					
Denial of Service	04-Jan-16	4.3	epan/dissectors/packet-dec-dnart.c in the DECnet NSP/RT dissector in Wireshark 1.10.12 through 1.10.14 mishandles a certain strdup return value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-3182***	https://bugzilla.redhat.com/show_bug.cgi?id=1219409	A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	epan/dissectors/packet-nbap.c in the NBAP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate conversation data, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet. ***Reference: CVE-2015-8711***	http://www.wireshark.org/security/wnpa-sec-2015-31.html	A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_hsdsch_channel_info function in epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 1.12.x before 1.12.9 does not validate the number of PDUs, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.		A-WIR-WIRES-181215/

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

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reference: CVE-2015-8712		
Denial of Service	04-Jan-16	4.3	epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 1.12.x before 1.12.9 does not properly reserve memory for channel ID mappings, which allows remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted packet. ***Reference: CVE-2015-8713***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_dcom_OBJREF function in epan/dissectors/packet-dcom.c in the DCOM dissector in Wireshark 1.12.x before 1.12.9 does not initialize a certain IPv4 data structure, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8714***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	epan/dissectors/packet-alljoyn.c in the AllJoyn dissector in Wireshark 1.12.x before 1.12.9 does not check for empty arguments, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet. ***Reference: CVE-2015-8715***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The init_t38_info_conv function in epan/dissectors/packet-t38.c in the T.38 dissector in Wireshark 1.12.x before 1.12.9 does not ensure that a conversation exists, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8716***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_sdp function in epan/dissectors/packet-sdp.c in the SDP dissector in Wireshark 1.12.x before 1.12.9 does not prevent use of a negative media count, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8717***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	Double free vulnerability in epan/dissectors/packet-nlm.c in the NLM dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1, when the "Match MSG/RES packets for async NLM" option is enabled,		A-WIR-WIRES-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8718***		
Denial of Service	04-Jan-16	4.3	The dissect_dns_answer function in epan/dissectors/packet-dns.c in the DNS dissector in Wireshark 1.12.x before 1.12.9 mishandles the EDNS0 Client Subnet option, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8719***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_ber_GeneralizedTime function in epan/dissectors/packet-ber.c in the BER dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 improperly checks an sscanf return value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8720***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	epan/dissectors/packet-sctp.c in the SCTP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the frame pointer, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet. ***Reference: CVE-2015-8722***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The AirPDcapDecryptWPABroadcastKey function in epan/crypt/airpdcap.c in the 802.11 dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not verify the WPA broadcast key length, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet. ***Reference: CVE-2015-8724***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	wiretap/vwr.c in the VeriWave file parser in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate certain signature and Modulation and Coding Scheme (MCS) data, which allows remote attackers to cause a denial of service (out-of-bounds read and application		A-WIR-WIRES-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			crash) via a crafted file. ***Reference: CVE-2015-8726***		
Denial of Service	04-Jan-16	4.3	The dissect_rsvp_common function in epan/dissectors/packet-rsvp.c in the RSVP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not properly maintain request-key data, which allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted packet. ***Reference: CVE-2015-8727***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The ascend_seek function in wiretap/ascendtext.c in the Ascend file parser in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not ensure the presence of a '\0' character at the end of a date string, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file. ***Reference: CVE-2015-8729***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	epan/dissectors/packet-nbap.c in the NBAP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the number of items, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted packet. ***Reference: CVE-2015-8730***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissct_rsl_ipaccess_msg function in epan/dissectors/packet-rsl.c in the RSL dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not reject unknown TLV types, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet. ***Reference: CVE-2015-8731***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_zcl_pwr_prof_pwrprofstatersp function in epan/dissectors/packet-zbee-zcl-general.c in the ZigBee ZCL dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the Total Profile Number field, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash)		A-WIR-WIRES-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			via a crafted packet. ***Reference: CVE-2015-8732***		
Denial of Service	04-Jan-16	4.3	The ngsniffer_process_record function in wiretap/ngsniffer.c in the Sniffer file parser in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the relationships between record lengths and record header lengths, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file. ***Reference: CVE-2015-8733***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_nwp function in epan/dissectors/packet-nwp.c in the NWP dissector in Wireshark 2.0.x before 2.0.1 mishandles the packet type, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8734***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The get_value function in epan/dissectors/packet-btatt.c in the Bluetooth Attribute (aka BT ATT) dissector in Wireshark 2.0.x before 2.0.1 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (invalid write operation and application crash) via a crafted packet. ***Reference: CVE-2015-8735***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The mp2t_open function in wiretap/mp2t.c in the MP2T file parser in Wireshark 2.0.x before 2.0.1 does not validate the bit rate, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted file. ***Reference: CVE-2015-8737***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The s7comm_decode_ud_cpu_szl_subfunc function in epan/dissectors/packet-s7comm_szl_ids.c in the S7COMM dissector in Wireshark 2.0.x before 2.0.1 does not validate the list count in an SZL response, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted packet.		A-WIR-WIRES-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reference: CVE-2015-8738		
Denial of Service	04-Jan-16	4.3	The ipmi_fmt_udpport function in epan/dissectors/packet-ipmi.c in the IPMI dissector in Wireshark 2.0.x before 2.0.1 improperly attempts to access a packet scope, which allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted packet. ***Reference: CVE-2015-8739***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_ppi function in epan/dissectors/packet-ppi.c in the PPI dissector in Wireshark 2.0.x before 2.0.1 does not initialize a packet-header data structure, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. ***Reference: CVE-2015-8741***		A-WIR-WIRES-181215/
Denial of Service	04-Jan-16	4.3	The dissect_CPMSetBindings function in epan/dissectors/packet-mswsp.c in the MS-WSP dissector in Wireshark 2.0.x before 2.0.1 does not validate the column size, which allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted packet. ***Reference: CVE-2015-8742***		A-WIR-WIRES-181215/
Denial of Service; Overflow	04-Jan-16	4.3	Buffer overflow in the tvb_uncompress function in epan/tvbuff_zlib.c in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 allows remote attackers to cause a denial of service (application crash) via a crafted packet with zlib compression. ***Reference: CVE-2015-8721***		A-WIR-WIRES-181215/
Denial of Service; Overflow	04-Jan-16	4.3	The AirPDcapPacketProcess function in epan/crypt/airpdcap.c in the 802.11 dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the relationship between the total length and the capture length, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet. ***Reference: CVE-2015-8723***		A-WIR-WIRES-181215/
Denial of Service; Overflow	04-Jan-16	4.3	The dissect_diameter_base_framed_ipv6_prefix function in		A-WIR-WIRES-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			epan/dissectors/packet-diameter.c in the DIAMETER dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the IPv6 prefix length, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet. ***Reference: CVE-2015-8725***		
Denial of Service; Overflow	04-Jan-16	4.3	The Mobile Identity parser in (1) epan/dissectors/packet-ansi_a.c in the ANSI A dissector and (2) epan/dissectors/packet-gsm_a_common.c in the GSM A dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 improperly uses the tvb_bcd_dig_to_wmem_packet_str function, which allows remote attackers to cause a denial of service (buffer overflow and application crash) via a crafted packet. ***Reference: CVE-2015-8728***		A-WIR-WIRES-181215/
Denial of Service; Overflow	04-Jan-16	4.3	The mp2t_find_next_pcr function in wiretap/mp2t.c in the MP2T file parser in Wireshark 2.0.x before 2.0.1 does not reserve memory for a trailer, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted file. ***Reference: CVE-2015-8736***		A-WIR-WIRES-181215/
Denial of Service; Overflow	04-Jan-16	4.3	The dissect_tds7_colmetadata_token function in epan/dissectors/packet-tds.c in the TDS dissector in Wireshark 2.0.x before 2.0.1 does not validate the number of columns, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet. ***Reference: CVE-2015-8740***		A-WIR-WIRES-181215/
Operating System (OS)					
Cisco					
Ios Xr *Cisco IOS XR Software is a modular and fully distributed network operating system for service provider networks.*					
Cross Site Scripting	05-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in HP StoreOnce Backup system software before 3.13.1 allows remote authenticated users to inject arbitrary web script or HTML via	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160104-iosxr	OS-CIS-IOS X-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			unspecified vectors. ***Reference: CVE-2015-5447***		
Denial of Service	04-Jan-16	5	Cisco IOS XR 4.2.0, 4.3.0, 5.0.0, 5.1.0, 5.2.0, 5.2.2, 5.2.4, 5.3.0, and 5.3.2 does not properly restrict the number of Path Computation Elements (PCEs) for OSPF LSA opaque area updates, which allows remote attackers to cause a denial of service (device reload) via a crafted update, aka Bug ID CSCuw83486. ***Reference: CVE-2015-6432***		OS-CIS-IOS X-181215/
Google					
Android *Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices*					
Gain Information	06-Jan-16	2.9	Bluetooth in Android 6.0 before 2016-01-01 allows remote attackers to obtain sensitive Contacts information by leveraging pairing, aka internal bug 23607427. ***Reference: CVE-2015-6641***	http://source.android.com/security/bulletin/2016-01-01.html	OS-GOO-ANDRO-181215/
Gain Information	06-Jan-16	3.3	Wi-Fi in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows remote attackers to obtain sensitive Wi-Fi information by leveraging access to the local physical environment, aka internal bug 25266660. ***Reference: CVE-2015-5310***		OS-GOO-ANDRO-181215/
Gain Information	06-Jan-16	4.3	Bouncy Castle in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information via a crafted application, aka internal bug 24106146. ***Reference: CVE-2015-6644***		OS-GOO-ANDRO-181215/
Denial of Service	06-Jan-16	7.1	SyncManager in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to cause a denial of service (continuous rebooting) via a crafted application, aka internal bug 23591205. ***Reference: CVE-2015-6645***		OS-GOO-ANDRO-181215/
Bypass	06-Jan-16	7.2	Setup Wizard in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows physically proximate attackers to modify settings or bypass a reset protection mechanism via unspecified vectors, aka internal bug 25290269. ***Reference: CVE-2015-6643***		OS-GOO-ANDRO-181215/
Bypass; Gain	06-Jan-16	7.8	The kernel in Android before 5.1.1		OS-GOO-

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Information			LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, via unknown vectors, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 24157888. ***Reference: CVE-2015-6642***		ANDRO-181215/
Denial of Service	06-Jan-16	7.8	The System V IPC implementation in the kernel in Android before 6.0 2016-01-01 allows attackers to cause a denial of service (global kernel resource consumption) by leveraging improper interaction between IPC resource allocation and the memory manager, aka internal bug 22300191, a different vulnerability than CVE-2015-7613. ***Reference: CVE-2015-6646***		OS-GOO-ANDRO-181215/
Gain Privileges	06-Jan-16	9.3	The MediaTek misc-sd driver in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application, aka internal bug 25307013. ***Reference: CVE-2015-6637***		OS-GOO-ANDRO-181215/
Gain Privileges	06-Jan-16	9.3	The Imagination Technologies driver in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application, aka internal bug 24673908. ***Reference: CVE-2015-6638***		OS-GOO-ANDRO-181215/
Gain Privileges	06-Jan-16	9.3	The Widevine QSEE TrustZone application in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application that leverages QSEECOM access, aka internal bug 24446875. ***Reference: CVE-2015-6639***		O-GOO-ANDRO-181215/
Gain Privileges	06-Jan-16	9.3	The Widevine QSEE TrustZone application in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application that leverages QSEECOM access, aka internal bug 24441554. ***Reference: CVE-2015-6647***		OS-GOO-ANDRO-181215/
Denial of Service; Gain	06-Jan-16	9.3	The prctl_set_vma_anon_name function in kernel/sys.c in Android		OS-GOO-ANDRO-

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Privileges			before 5.1.1 LMY49F and 6.0 before 2016-01-01 does not ensure that only one vma is accessed in a certain update action, which allows attackers to gain privileges or cause a denial of service (vma list corruption) via a crafted application, aka internal bug 20017123. ***Reference: CVE-2015-6640***		181215/
Denial of Service; Execute Code; Overflow; Memory Corruption	06-Jan-16	10	mediaserver in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bugs 25070493 and 24686670. ***Reference: CVE-2015-6636***		OS-GOO-ANDRO-181215/
HP					
Network Switch Software *It is an approach to computer networking that allows network administrators to manage network services through abstraction of higher-level functionality.*					
Bypass	05-Jan-16	4.6	HPE Network Switches with software 15.16.x and 15.17.x allow local users to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-6860. ***Reference: CVE-2015-6859***	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04920918	OS-HP-NETWO-181215/
Storeonce Backup System Software *Simple, affordable and flexible protection with rapid recovery and application integration*					
Execute Code	05-Jan-16	5.8	HP StoreOnce Backup system software before 3.13.1 allows remote attackers to execute arbitrary code via unspecified vectors. ***Reference: CVE-2015-5446***	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04858589	OS-HP-STORE-181215/
Cross-site Request Forgery	05-Jan-16	6.8	Cross-site request forgery (CSRF) vulnerability in HP StoreOnce Backup system software before 3.13.1 allows remote authenticated users to hijack the authentication of unspecified victims via unknown vectors. ***Reference: CVE-2015-5445***		OS-HP-STORE-181215/
IBM					
Security Access Manager 9.0 Firmware; Security Access Manager For Web 7.0 Firmware *The IBM Security Access Manager virtual appliance helps organizations secure and manage mobile user access and protect mobile applications against fraudulent unauthorized access.*					
Execute Code	02-Jan-16	8.5	IBM Security Access Manager for Web 7.0.0 before FP19 and 8.0 before 8.0.1.3 IF3, and Security Access Manager 9.0 before 9.0.0.0 IF1, allows remote authenticated users to execute arbitrary OS commands by	http://www-01.ibm.com/support/docview.wss?uid=swg21970510	OS-IBM-SECUR-181215/

Product / Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			leveraging Local Management Interface (LMI) access. ***Reference: CVE-2015-5018***		