National Critical Information Infrastructure Protection Centre

CVE Report

01- 15 April 2016 **Vol. 3 No.6**

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Application (A)					
9bis;Simon Tatham					
Kitty/Putty *KiTTY is a fork of the popular PuTTY telnet and SSH client packaged as a portable app, so you can connect in to your systems on the go.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	07-April-16	7.5	Stack-based buffer overflow in the SCP command-line utility in PuTTY before 0.67 and KiTTY 0.66.6.3 and earlier allows remote servers to cause a denial of service (stack memory corruption) or execute arbitrary code via a crafted SCP-SINK file-size response to an SCP download request. **Reference: CVE-2016-2563**	http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-pscp-sink-sscanf.html	A-9BI-KITTY-250416/1
Adobe					
Creative Cloud *Adobe Creative Cloud is a software as a service offering from Adobe Systems that gives users access to a collection of software developed by Adobe for graphic design, video editing, web development, photography, and cloud services.*					
Not Avialable	12-April-16	9.4	The Sync Process in the JavaScript API for Creative Cloud Libraries in Adobe Creative Cloud Desktop Application before 3.6.0.244 allows remote attackers to read or write to arbitrary files via unspecified vectors. **Reference: CVE-2016-1034**	https://helpx.adobe.com/security/products/creative-cloud/apsb16-11.html	A-ADO-CREAT-250416/2
Robohelp *RoboHelp is a help authoring tool (HAT).*					
Gain Information	12-April-16	5	Adobe RoboHelp Server 9 before 9.0.1 mishandles SQL queries, which allows attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-1035**	https://helpx.adobe.com/security/products/robohelp-server/apsb16-12.html	A-ADO-ROBOH-250416/3

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

Apache

Activemq

Apache ActiveMQ is the most popular and powerful open source messaging and Integration Patterns server.

Not Available	07-April-16	4.3	The web-based administration console in Apache ActiveMQ 5.x before 5.13.2 does not send an X-Frame-Options HTTP header, which makes it easier for remote attackers to conduct clickjacking attacks via a crafted web page that contains a (1) FRAME or (2) IFRAME element. **Reference: CVE-2016-0734**	http://activemq.apache.org/security-advisories.data/CVE-2016-0734-announcement.txt	A-APA-ACTIV-250416/4

Apache Directory Studio;Apache Ldap Studio

LDAP Studio is a complete LDAP tooling platform intended to be used with any LDAP server however it is particularly designed for use with the Apache Directory.

Execute Code	11-April-16	9.3	The CSV export in Apache LDAP Studio and Apache Directory Studio before 2.0.0-M10 does not properly escape field values, which might allow attackers to execute arbitrary commands by leveraging a crafted LDAP entry that is interpreted as a formula when imported into a spreadsheet. **Reference: CVE-2015-5349**	https://directory.apache.org/studio/news.html	A-APA-APACH-250416/5

Jetspeed

Jetspeed is an Open Portal Platform and Enterprise Information Portal, written entirely in open source under the Apache license in Java.

Not Available	11-April-16	6.4	The User Manager service in Apache Jetspeed before 2.3.1 does not properly restrict access using Jetspeed Security, which allows remote attackers to (1) add, (2) edit, or (3) delete users via the REST API. **Reference: CVE-2016-2171**	https://portals.apache.org/jetspeed-2/security-reports.html#CVE-2016-2171	A-APA-JETSP-250416/6

Ofbiz

Open source enterprise automation software project.

Cross Site Scripting	12-April-16	4.3	Cross-site scripting (XSS) vulnerability in the DisplayEntityField.getDescription method in	http://ofbiz.apache.org/download.html#vulnerabilities	A-APA-OFBIZ-250416/7

			ModelFormField.java in Apache OFBiz before 12.04.06 and 13.07.x before 13.07.03 allows remote attackers to inject arbitrary web script or HTML via the description attribute of a display-entity element. **Reference: CVE-2015-3268**		
Execute Code	12-April-16	7.5	Apache OFBiz 12.04.x before 12.04.06 and 13.07.x before 13.07.03 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library. **Reference: CVE-2016-2170**	https://blogs.apache.org/ofbiz/entry/announce_apache_ofbiz_12_04	A-APA-OFBIZ-250416/8

Openmeetings

OpenMeetings is software used for presenting, online training, web conferencing, collaborative whiteboard drawing and document editing, and user desktop sharing.

Directory Traversal	11-April-16	4	Directory traversal vulnerability in the Import/Export System Backups functionality in Apache OpenMeetings before 3.1.1 allows remote authenticated administrators to write to arbitrary files via a .. (dot dot) in a ZIP archive entry. **Reference: CVE-2016-0784**	https://www.apache.org/dist/openmeetings/3.1.1/CHANGELOG	A-APA-OPENM-250416/9
Cross Site Scripting	11-April-16	4.3	Cross-site scripting (XSS) vulnerability in Apache OpenMeetings before 3.1.1 allows remote attackers to inject arbitrary web script or HTML via the event description when creating an event. **Reference: CVE-2016-2163**	http://openmeetings.apache.org/security.html	A-APA-OPENM-250416/10
Gain Information	11-April-16	5	The (1) FileService.importFileByInternalUserId and (2) FileService.importFile SOAP API methods in Apache OpenMeetings before 3.1.1 improperly use the Java URL class without checking the specified protocol handler,	https://www.apache.org/dist/openmeetings/3.1.1/CHANGELOG	A-APA-OPENM-250416/11

			which allows remote attackers to read arbitrary files by attempting to upload a file. **Reference: CVE-2016-2164**		
Gain Information	11-April-16	5	The sendHashByUser function in Apache OpenMeetings before 3.1.1 generates predictable password reset tokens, which makes it easier for remote attackers to reset arbitrary user passwords by leveraging knowledge of a user name and the current system time. **Reference: CVE-2016-0783**	https://www.apache.org/dist/openmeetings/3.1.1/CHANGELOG	A-APA-OPENM-250416/12
Qpid Proton *Qpid Proton is a high-performance, lightweight messaging library.*					
Gain Information	12-April-16	5.8	The (1) proton.reactor.Connector, (2) proton.reactor.Container, and (3) proton.utils.BlockingConnection classes in Apache Qpid Proton before 0.12.1 improperly use an unencrypted connection for an amqps URI scheme when SSL support is unavailable, which might allow man-in-the-middle attackers to obtain sensitive information or modify data via unspecified vectors. **Reference: CVE-2016-2166**	https://git-wip-us.apache.org/repos/asf?p=qpid-proton.git;h=a058585	A-APA-QPID-250416/13
Ranger *Apache Ranger. Ranger is a framework to enable, monitor and manage comprehensive data security across the Hadoop platform.*					
Bypass	12-April-16	4	The Policy Admin Tool in Apache Ranger before 0.5.1 allows remote authenticated users to bypass intended access restrictions via the REST API. **Reference: CVE-2015-5167**	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-250416/14
Cross Site Scripting	11-April-16	4.3	Cross-site scripting (XSS) vulnerability in the Policy Admin Tool in Apache Ranger before 0.5.0 allows remote attackers to inject arbitrary web script or HTML via the HTTP User-Agent	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-250416/15

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

			header. **Reference: CVE-2015-0265**		
Bypass	11-April-16	6.5	Apache Ranger 0.5.x before 0.5.2 allows remote authenticated users to bypass intended parent resource-level access restrictions by leveraging mishandling of a resource-level exclude policy. **Reference: CVE-2016-0735**	http://mail-archives.apache.org/mod_mbox/ranger-dev/201603.mbox/%3CD31EE434.14B879%25vel%40apache.org%3E	A-APA-RANGE-250416/16
Bypass	11-April-16	6.5	The Policy Admin Tool in Apache Ranger before 0.5.0 allows remote authenticated users to bypass intended access restrictions via direct access to module URLs. **Reference: CVE-2015-0266**	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-250416/17
Bypass	12-April-16	7.5	The Admin UI in Apache Ranger before 0.5.1 does not properly handle authentication requests that lack a password, which allows remote attackers to bypass authentication by leveraging knowledge of a valid username. **Reference: CVE-2016-0733**	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-250416/18

Struts

Apache Struts is a discontinued 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.

Cross Site Scripting	12-April-16	4.3	Cross-site scripting (XSS) vulnerability in the URLDecoder function in JRE before 1.8, as used in Apache Struts 2.x before 2.3.28, when using a single byte page encoding, allows remote attackers to inject arbitrary web script or HTML via multi-byte characters in a url-encoded parameter. **Reference: CVE-2016-4003**	https://issues.apache.org/jira/browse/WW-4507	A-APA-STRUT-250416/19
Cross Site Scripting	12-April-16	4.3	Apache Struts 2.x before 2.3.25 does not sanitize text in the Locale object constructed by	http://struts.apache.org/docs/s2-030.html	A-APA-STRUT-250416/20

			I18NInterceptor, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors involving language display. **Reference: CVE-2016-2162**		
Execute Code	12-April-16	10	Apache Struts 2.x before 2.3.28 allows remote attackers to execute arbitrary code via a "%{}" sequence in a tag attribute, aka forced double OGNL evaluation. **Reference: CVE-2016-0785**	http://struts.apache.org/docs/s2-029.html	A-APA-STRUT-250416/21
Wicket *Lightweight component-based web application framework for the Java programming language.*					
Cross Site Scripting	12-April-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the (1) RadioGroup and (2) CheckBoxMultipleChoice classes in Apache Wicket 1.5.x before 1.5.15, 6.x before 6.22.0, and 7.x before 7.2.0 allow remote attackers to inject arbitrary web script or HTML via a crafted "value" attribute in a <input> element. **Reference: CVE-2015-7520**	http://wicket.apache.org/news/2016/03/02/cve-2015-7520.html	A-APA-WICKE-250416/22
Cross Site Scripting	12-April-16	4.3	Cross-site scripting (XSS) vulnerability in the getWindowOpenJavaScript function in org.apache.wicket.extensions.ajax.markup.html.modal.ModalWindow in Apache Wicket 1.5.x before 1.5.15, 6.x before 6.22.0, and 7.x before 7.2.0 might allow remote attackers to inject arbitrary web script or HTML via a ModalWindow title. **Reference: CVE-2015-5347**	https://issues.apache.org/jira/browse/WICKET-6037	A-APA-WICKE-250416/23
Xerces-c\+\+ *Xerces-C++ is a validating XML parser written in a portable subset of C++. Xerces-C++ makes it easy to give your application the ability to read and write XML.*					
Denial of Service;Exe	07-April-16	7.5	Multiple buffer overflows in (1) internal/XMLReader.cpp, (2)	https://issues.apache.org/jira/bro	A-APA-XERCE-

cute Code;Overflow;Memory Corruption			util/XMLURL.cpp, and (3) util/XMLUri.cpp in the XML Parser library in Apache Xerces-C before 3.1.3 allow remote attackers to cause a denial of service (segmentation fault or memory corruption) or possibly execute arbitrary code via a crafted document. **Reference: CVE-2016-0729**	wse/XERCESC-2061	250416/24

Atlassian

Confluence

Confluence is team collaboration software. Written in Java and mainly used in corporate environments, it is developed and marketed by Atlassian.

Gain Information	11-April-16	4	Atlassian Confluence before 5.8.17 allows remote authenticated users to read configuration files via the decoratorName parameter to (1) spaces/viewdefaultdecorator.action or (2) admin/viewdefaultdecorator.action. **Reference: CVE-2015-8399**	http://www.securityfocus.com/archive/1/archive/1/537232/100/0/threaded	A-ATL-CONFL-250416/25
Cross Site Scripting	11-April-16	4.3	Cross-site scripting (XSS) vulnerability in Atlassian Confluence before 5.8.17 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to rest/prototype/1/session/check. **Reference: CVE-2015-8398**	http://www.securityfocus.com/archive/1/archive/1/537232/100/0/threaded	A-ATL-CONFL-250416/26

Avast

Avast

Avast Software is a Czech security software company headquartered in Prague, Czech Republic, that develops antivirus software and internet security services.

Denial of Service;Execute Code;Overflow;Memory Corruption	11-April-16	9.3	Avast allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via a crafted PE file, related to authenticode parsing. **Reference: CVE-2016-3986**		A-AVA-AVAST-250416/27

CA

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

Api Gateway

API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

Not Available	05-April-16	6.4	CRLF injection vulnerability in CA API Gateway (formerly Layer7 API Gateway) 7.1 before 7.1.04, 8.0 through 8.3 before 8.3.01, and 8.4 before 8.4.01 allows remote attackers to have an unspecified impact via unknown vectors. **Reference: CVE-2016-3118**	http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/security-notices/ca20160405-01-security-notice-for-ca-api-gateway.aspx	A-CA-APIG-250416/28

Cacti

Cacti

Cacti is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality.

Execute Code; Sql Injection	11-April-16	6.5	SQL injection vulnerability in graph_view.php in Cacti 0.8.8.g allows remote authenticated users to execute arbitrary SQL commands via the host_group_data parameter. **Reference: CVE-2016-3659**		A-CAC-CACTI-250416/29
Execute Code; Sql Injection	11-April-16	6.5	SQL injection vulnerability in the host_new_graphs function in graphs_new.php in Cacti 0.8.8f and earlier allows remote authenticated users to execute arbitrary SQL commands via the cg_g parameter in a save action. **Reference: CVE-2015-8604**		A-CAC-CACTI-250416/30
Execute Code; Sql Injection	12-April-16	6.5	SQL injection vulnerability in tree.php in Cacti 0.8.8g and earlier allows remote authenticated users to execute arbitrary SQL commands via the parent_id parameter in an item_edit action. **Reference: CVE-2016-3172**		A-CAC-CACTI-250416/31

Cisco

Evolved Programmable Network Manager;Prime Infrastructure

Cisco Evolved Programmable Network Manager provides simplified, converged, multilayer management of carrier-grade networks of all sizes.

Cisco Prime Infrastructure simplifies the management of wireless and wired networks. It offers Day 0 and 1 provisioning, as well as Day N assurance from the branch to the data center.

Gain Privileges; Bypass	06-April-16	5.5	The web API in Cisco Prime Infrastructure 1.2.0 through 2.2(2) and Cisco Evolved Programmable Network Manager (EPNM) 1.2 allows remote authenticated users to bypass intended RBAC restrictions and gain privileges via an HTTP request that is inconsistent with a pattern filter, aka Bug ID CSCuy10227. **Reference: CVE-2016-1290**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-privauth	A-CIS-EVOLV-250416/32
Execute Code	06-April-16	9.3	Cisco Prime Infrastructure 1.2.0 through 2.2(2) and Cisco Evolved Programmable Network Manager (EPNM) 1.2 allow remote attackers to execute arbitrary code via crafted deserialized data in an HTTP POST request, aka Bug ID CSCuw03192. **Reference: CVE-2016-1291**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-remcode	A-CIS-EVOLV-250416/33

Ip Interoperability And Collaboration System

Cisco IP Interoperability and Collaboration System (IPICS) can simplify radio dispatch operations and improve response to incidents, emergencies, and facility events.

Cross Site Scripting	08-April-16	4.3	Cross-site scripting (XSS) vulnerability in Cisco IP Interoperability and Collaboration System 4.10(1) allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCuy12339. **Reference: CVE-2016-1375**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160407-cic	A-CIS-IP IN-250416/34

Unity Connection

Unity Connection is a robust unified messaging and voicemail solution that provides users with flexible message access options and IT with management simplicity.

Cross Site Scripting	12-April-16	4.3	Cross-site scripting (XSS) vulnerability in Cisco Unity Connection through 11.0 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters, aka Bug ID CSCus21776.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160412-unity	A-CIS-UNITY-250416/35

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-2016-1377		

Citrix

Xenmobile Server

XenMobile is enterprise mobility management software developed by Citrix.The product allows businesses to manage employee mobile devices and mobile applications. The software's aim is to increase productivity by allowing employees to securely work on both enterprise-owned and personal mobile devices and apps.

Cross Site Scripting	07-April-16	4.3	Cross-site scripting (XSS) vulnerability in the Web User Interface in Citrix XenMobile Server 10.0, 10.1 before Rolling Patch 4, and 10.3 before Rolling Patch 1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-2789**	http://support.citrix.com/article/CTX207499	A-CIT-XENMO-250416/36

Claws-mail

Claws-mail

Claws Mail is a free and open source, GTK+-based email and news client. It offers easy configuration and an abundance of features.

Overflow	11-April-16	7.5	Stack-based buffer overflow in the conv_euctojis function in codeconv.c in Claws Mail 3.13.1 allows remote attackers to have unspecified impact via a crafted email, involving Japanese character set conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8614. **Reference: CVE-2015-8708**	http://www.openwall.com/lists/oss-security/2015/12/31/1	A-CLA-CLAWS-250416/37

Cloudbees

Jenkins

Jenkins is an open source continuous integration tool written in Java.

Http R.Spl.	07-April-16	4.3	CRLF injection vulnerability in the CLI command documentation in CloudBees Jenkins before 1.650 and LTS before 1.642.2 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. **Reference: CVE-2016-0789**	https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-02-24	A-CLO-JENKI-250416/38
Not	07-April-	5	CloudBees Jenkins before 1.650	https://wiki.jenki	A-CLO-

Available	16		and LTS before 1.642.2 do not use a constant-time algorithm to verify API tokens, which makes it easier for remote attackers to determine API tokens via a brute-force approach. **Reference: CVE-2016-0790**	ns-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-02-24	JENKI-250416/39
Bypass; Gain Information; Cross-site Request Forgery	07-April-16	7.5	CloudBees Jenkins before 1.650 and LTS before 1.642.2 do not use a constant-time algorithm to verify CSRF tokens, which makes it easier for remote attackers to bypass a CSRF protection mechanism via a brute-force approach. **Reference: CVE-2016-0791**	https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-02-24	A-CLO-JENKI-250416/40
Execute Code	07-April-16	9	Multiple unspecified API endpoints in CloudBees Jenkins before 1.650 and LTS before 1.642.2 allow remote authenticated users to execute arbitrary code via serialized data in an XML file, related to XStream and groovy.util.Expando. **Reference: CVE-2016-0792**	https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-02-24	A-CLO-JENKI-250416/41
Execute Code	07-April-16	10	The remoting module in CloudBees Jenkins before 1.650 and LTS before 1.642.2 allows remote attackers to execute arbitrary code by opening a JRMP listener. **Reference: CVE-2016-0788**	https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2016-02-24	A-CLO-JENKI-250416/42

Drupal

Drupal

Drupal is content management software. It's used to make many of the websites and applications you use every day.

Bypass	12-April-16	5	The Form API in Drupal 6.x before 6.38 ignores access restrictions on submit buttons, which might allow remote attackers to bypass intended access restrictions by leveraging permission to submit a form with a button that has	https://www.drupal.org/SA-CORE-2016-001	A-DRU-DRUPA-250416/43

			"#access" set to FALSE in the server-side form definition. **Reference: CVE-2016-3165**		

EMC

Documentum D2

EMC Documentum D2 is the advanced, intuitive, and configurable content-centric client for Documentum that accelerates adoption of ECM applications.

Not Available	07-April-16	9	EMC Documentum D2 before 4.6 lacks intended ACLs for configuration objects, which allows remote authenticated users to modify objects via unspecified vectors. **Reference: CVE-2016-0888**	http://seclists.org/bugtraq/2016/Apr/20	A-EMC-DOCUM-250416/44

Eset

Nod32

ESET Nod32 Antivirus - one of the best virus protection Softwares in the world.

Execute Code; Overflow	11-April-16	10	Heap-based buffer overflow in the Archive support module in ESET NOD32 before update 11861 allows remote attackers to execute arbitrary code via a large number of languages in an EPOC installation file of type SIS_FILE_MULTILANG. **Reference: CVE-2015-8841**	http://www.virusradar.com/en/update/info/11861	A-ESE-NOD32-250416/45

Exim

Exim

Exim is a mail transfer agent (MTA) used on Unix-like operating systems. Exim is free software distributed under the terms of the GNU General Public License.

Gain Privileges	07-April-16	6.9	Exim before 4.86.2, when installed setuid root, allows local users to gain privileges via the perl_startup argument. **Reference: CVE-2016-1531**	http://www.exim.org/static/doc/CVE-2016-1531.txt	A-EXI-EXIM-250416/46

F5

Big-ip Access Policy Manager;Big-ip Edge Gateway

BIG-IP Access Policy Manager (APM) is a flexible, high-performance access and security solution that provides unified global access to your business.

F5 BIG-IP Edge Gateway is an accelerated remote access solution that brings together SSL VPN, security, application acceleration, and availability services.

Gain Information	13-April-16	4.3	The Single Sign-On (SSO) feature in F5 BIG-IP APM 11.x before 11.6.0 HF6 and BIG-IP Edge Gateway 11.0.0 through	https://support.f5.com/kb/en-us/solutions/public/k/82/sol826790	A-F5-BIG-I-250416/47

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

			11.3.0 might allow remote attackers to obtain sensitive SessionId information by leveraging access to the Location HTTP header in a redirect. **Reference: CVE-2016-3686**	59.html	

Foxitsoftware

Foxit Reader

Foxit Reader is a lightweight, fast, and secure PDF Reader capable of high-volume processing.

Overflow; Gain Privileges; Memory Corruption	13-April-16	6.9	The Foxit Cloud Update Service (FoxitCloudUpdateService) in Foxit Reader 6.1 through 6.2.x and 7.x before 7.2.2, when an update to the Cloud plugin is available, allows local users to gain privileges by writing crafted data to a shared memory region, which triggers memory corruption. **Reference: CVE-2015-8843**	https://www.foxitsoftware.com/support/security-bulletins.php#FRD-35	A-FOX-FOXIT-250416/48

Google;Redhat

Kubernetes/Openshift

Kubernetes is a container management system meant to be deployed on Docker-capable clustered environments. OpenShift is an open source PaaS by Red Hat based on top of Docker containers and the Kubernetes container cluster manager for enterprise app development.

Gain Information	11-April-16	5	Kubernetes before 1.2.0-alpha.5 allows remote attackers to read arbitrary pod logs via a container name. **Reference: CVE-2015-7528**	https://github.com/kubernetes/kubernetes/releases/tag/v1.2.0-alpha.5	A-GOO-KUBER-250416/49

HP

Asset Manager;Asset Manager Cloudsystem Chargeback

Asset management is the management of a client's investments by a financial services company, usually an investment bank.

It measure the financial effectiveness of your private and hybrid cloud services.

Execute Code	05-April-16	7.5	HPE Asset Manager 9.40, 9.41, and 9.50 and Asset Manager CloudSystem Chargeback 9.40 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library. **Reference: CVE-2016-2000**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05064889	A-HP-ASSET-250416/50

IBM

Maximo Asset Management

IBM Maximo Asset Management is an enterprise asset management (EAM) software solution product produced by IBM. It is a solution which is used to operate, maintain and dispose of enterprise assets.

Bypass	05-April-16	4	shiprec.xml in the SHIPREC application in IBM Maximo Asset Management 7.1 and 7.5 before 7.5.0.10 and 7.6 before 7.6.0.4 allows remote authenticated users to bypass intended item-selection restrictions via unspecified vectors. **Reference: CVE-2016-0289**	http://www-01.ibm.com/support/docview.wss?uid=swg21979519	A-IBM-MAXIM-250416/51

Tivoli Storage Manager Fastback

Tivoli Storage Manager FastBack for Workstations simplifies the backup and recovery of valuable information on your employees' personal computers.

Denial of Service	05-April-16	5	The server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to cause a denial of service (service crash) via crafted packets to a TCP port. **Reference: CVE-2015-8523**	http://www-01.ibm.com/support/docview.wss?uid=swg21975536	A-IBM-TIVOL-250416/52
Execute Code; Overflow	05-April-16	7.5	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8520, and CVE-2015-8521. **Reference: CVE-2015-8522**	http://www-01.ibm.com/support/docview.wss?uid=swg21975536	A-IBM-TIVOL-250416/53
Execute Code; Overflow	05-April-16	7.5	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8520, and CVE-2015-8522. **Reference: CVE-2015-8521**	http://www-01.ibm.com/support/docview.wss?uid=swg21975536	A-IBM-TIVOL-250416/54
Execute	05-April-	7.5	Buffer overflow in the server in	http://www-	A-IBM-

Code; Overflow	16		IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8521, and CVE-2015-8522. **Reference: CVE-2015-8520**	01.ibm.com/support/docview.wss?uid=swg21975536	TIVOL-250416/55
Execute Code; Overflow	05-April-16	7.5	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8520, CVE-2015-8521, and CVE-2015-8522. **Reference: CVE-2015-8519**	http://www-01.ibm.com/support/docview.wss?uid=swg21975536	A-IBM-TIVOL-250416/56

Iconics

Webhmi

Webhmi uses a Web browser, such as Microsoft Edge, Internet Explorer, Google Chrome, Safari or Firefox, to provide an interface with ICONICS' graphics, trending and alarming applications (applications within the HMI/SCADA suites).

Directory Traversal	01-April-16	5	Directory traversal vulnerability in ICONICS WebHMI 9 and earlier allows remote attackers to read configuration files, and consequently discover password hashes, via unspecified vectors. **Reference: CVE-2016-2289**	https://ics-cert.us-cert.gov/advisories/ICSA-16-091-01	A-ICO-WEBHM-250416/57

Mantisbt

Mantisbt

Mantis Bug Tracker is a free and open source, web-based bug tracking system released under the terms of the GNU General Public License version 2.

Gain Information	11-April-16	5	Incomplete blacklist vulnerability in the config_is_private function in config_api.php in MantisBT 1.3.x before 1.3.0 allows remote attackers to obtain sensitive master salt configuration information via a SOAP API request. **Reference: CVE-2014-9759**	https://mantisbt.org/bugs/view.php?id=20277	A-MAN-MANTI-250416/58

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

Mcafee

Advanced Threat Defense

McAfee Advanced Threat Defense detects targeted attacks and connects with existing defenses, converting threat intelligence into immediate action and protection.

Bypass	08-April-16	5	McAfee Advanced Threat Defense (ATD) before 3.4.8.178 might allow remote attackers to bypass malware detection by leveraging information about the parent process. **Reference: CVE-2016-3983**	https://kc.mcafee.com/corporate/index?page=content&id=SB10149	A-MCA-ADVAN-250416/59

Email Gateway

Email Gateway helps you boost your email security and consolidate your defenses with inbound threat protection, outbound data loss prevention, encryption.

Cross Site Scripting	06-April-16	4.3	Cross-site scripting (XSS) vulnerability in McAfee Email Gateway (MEG) 7.6.x before 7.6.404, when File Filtering is enabled with the action set to ESERVICES:REPLACE, allows remote attackers to inject arbitrary web script or HTML via an attachment in a blocked email. **Reference: CVE-2016-3969**	https://kc.mcafee.com/corporate/index?page=content&id=SB10153	A-MCA-EMAIL-250416/60

Microsoft

net Framework

Software framework developed by Microsoft that runs primarily on Microsoft Windows.

Execute Code; Gain Privileges	12-April-16	7.2	Microsoft .NET Framework 4.6 and 4.6.1 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ".NET Framework Remote Code Execution Vulnerability." **Reference: CVE-2016-0148**	http://technet.microsoft.com/en-us/security/bulletin/ms16-041	A-MIC-.NET-250416/61

Edge

EDGE Software Inc. is a custom software services firm based in Austin, TX.

Bypass	12-April-16	4.3	Microsoft Edge allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Edge Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0158.	http://technet.microsoft.com/en-us/security/bulletin/ms16-038	A-MIC-EDGE-250416/62

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-2016-0161		
Bypass	12-April-16	4.3	Microsoft Edge allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Edge Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0161.	http://technet.microsoft.com/en-us/security/bulletin/ms16-038	A-MIC-EDGE-250416/63
			Reference: CVE-2016-0158		
Denial of Service;Execute Code;Overflow;Memory Corruption	12-April-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0156.	http://technet.microsoft.com/en-us/security/bulletin/ms16-038	A-MIC-EDGE-250416/64
			Reference: CVE-2016-0157		
Denial of Service;Execute Code;Overflow;Memory Corruption	12-April-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0157.	http://technet.microsoft.com/en-us/security/bulletin/ms16-038	A-MIC-EDGE-250416/65
			Reference: CVE-2016-0156		
Denial of Service;Execute Code;Overflow;Memory Corruption	12-April-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0156 and CVE-2016-0157.	http://technet.microsoft.com/en-us/security/bulletin/ms16-038	A-MIC-EDGE-250416/66
			Reference: CVE-2016-0155		
Excel;Excel Viewer;Word For Mac					
The Microsoft Excel Viewer is a small, freely redistributable program that lets you view and print Microsoft Excel spreadsheets if you don't have Excel installed.					
Execute Code;Overflow;Memory	12-April-16	9.3	Microsoft Excel 2010 SP2, Word for Mac 2011, and Excel Viewer allow remote attackers to	http://technet.microsoft.com/en-us/security/bulletin/ms16-038	A-MIC-EXCEL-250416/67

Corruption			execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-0139**	in/ms16-042	

Excel;Office Compatibility Pack;Sharepoint Designer;Sharepoint Foundation

Microsoft Office Compatibility Pack is an add-on for Microsoft Office 2000, Office XP and Office 2003.

Microsoft SharePoint Designer (SPD), formerly known as Microsoft Office SharePoint Designer, is a discontinued HTML editor freeware specialized in creating or modifying Microsoft SharePoint sites, workflows and web pages.

Execute Code;Overflow;Memory Corruption	12-April-16	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-0136**	http://technet.microsoft.com/en-us/security/bulletin/ms16-042	A-MIC-EXCEL-250416/68

Internet Explorer

Internet Explorer is a series of graphical web browsers developed by Microsoft.

Gain Information	12-April-16	4.3	Microsoft Internet Explorer 9 through 11 allows remote attackers to determine the existence of files via crafted JavaScript code, aka "Internet Explorer Information Disclosure Vulnerability." **Reference: CVE-2016-0162**	http://technet.microsoft.com/en-us/security/bulletin/ms16-037	A-MIC-INTER-250416/69
Execute Code; Gain Privileges	12-April-16	7.2	Microsoft Internet Explorer 11 mishandles DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability." **Reference: CVE-2016-0160**	http://technet.microsoft.com/en-us/security/bulletin/ms16-037	A-MIC-INTER-250416/70
Denial of Service;Execute Code;Overflow;Memory	12-April-16	7.6	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web	http://technet.microsoft.com/en-us/security/bulletin/ms16-037	A-MIC-INTER-250416/71

Corruption			site, aka "Internet Explorer Memory Corruption Vulnerability." **Reference: CVE-2016-0166**		
Denial of Service;Execute Code;Overflow;Memory Corruption	12-April-16	7.6	Microsoft Internet Explorer 10 and 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-2016-0164**	http://technet.microsoft.com/en-us/security/bulletin/ms16-037	A-MIC-INTER-250416/72
Denial of Service;Execute Code;Overflow;Memory Corruption	12-April-16	7.6	Microsoft Internet Explorer 9 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-2016-0159**	http://technet.microsoft.com/en-us/security/bulletin/ms16-037	A-MIC-INTER-250416/73
Xml Core Services *A set of services that allow applications written in JScript, VBScript, and Microsoft development tools to build Windows-native XML-based applications.*					
Execute Code	12-April-16	9.3	Microsoft XML Core Services 3.0 allows remote attackers to execute arbitrary code via a crafted web site, aka "MSXML 3.0 Remote Code Execution Vulnerability." **Reference: CVE-2016-0147**	http://technet.microsoft.com/en-us/security/bulletin/ms16-040	A-MIC-XMLC-250416/74
Openstack					
Image Registry And Delivery Service (glance) *The Glance project provides services for discovering, registering, and retrieving virtual machine images.*					
Not Available	13-April-16	4	OpenStack Image Service (Glance) before 2015.1.3 (kilo) and 11.0.x before 11.0.2 (liberty), when show_multiple_locations is enabled, allow remote authenticated users to change image status and upload new image data by removing the last location of an image.	https://security.openstack.org/ossa/OSSA-2016-006.html	A-OPE-IMAGE-250416/75

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-2016-0757		

Tripleo Heat Templates

TripleO is a program aimed at installing, upgrading and operating OpenStack clouds using OpenStack's own cloud facilities as the foundations - building on nova, neutron and heat to automate fleet management at datacentre scale (and scaling down to as few as 2 machines).

Not Available	11-April-16	5	The TripleO Heat templates (tripleo-heat-templates), when deployed via the commandline interface, allow remote attackers to spoof OpenStack Networking metadata requests by leveraging knowledge of the default value of the NeutronMetadataProxySharedSecret parameter. **Reference: CVE-2015-5303**	https://bugs.launchpad.net/tripleo/+bug/1516027	A-OPE-TRIPL-250416/76

OTR

Pidgin-otr

OTR (Off-the-record) is a protocol that allows users of instant messaging or chat tools to have conversations that are confidential.

Execute Code	11-April-16	10	Use-after-free vulnerability in the create_smp_dialog function in gtk-dialog.c in the Off-the-Record Messaging (OTR) pidgin-otr plugin before 4.0.2 for Pidgin allows remote attackers to execute arbitrary code via vectors related to the "Authenticate buddy" menu item. **Reference: CVE-2015-8833**	https://bugs.otr.im/issues/128	A-OTR-PIDGI-250416/77

Postgresql

Postgresql

PostgreSQL, often simply Postgres, is an object-relational database management system (ORDBMS) with an emphasis on extensibility.

Bypass	11-April-16	5	PostgreSQL before 9.5.x before 9.5.2 does not properly maintain row-security status in cached plans, which might allow attackers to bypass intended access restrictions by leveraging a session that performs queries as more than one role. **Reference: CVE-2016-2193**	http://git.postgresql.org/gitweb/?p=postgresql.git;a=commitdiff;h=db69e58a0642ef7fa46d62f6c4cf2460c3a1b41b	A-POS-POSTG-250416/78

Denial of Service; Bypass; Gain Information	11-April-16	8.5	The (1) brin_page_type and (2) brin_metapage_info functions in the pageinspect extension in PostgreSQL before 9.5.x before 9.5.2 allows attackers to bypass intended access restrictions and consequently obtain sensitive server memory information or cause a denial of service (server crash) via a crafted bytea value in a BRIN index page. **Reference: CVE-2016-3065**	http://www.postgresql.org/docs/current/static/release-9-5-2.html	A-POS-POSTG-250416/79

Prepopulate Project

Prepopulate

The Prepopulate module allows fields in most forms to be pre-populated from the $_REQUEST variable.

Not Available	08-April-16	7.5	The _prepopulate_request_walk function in the Prepopulate module 7.x-2.x before 7.x-2.1 for Drupal allows remote attackers to modify the (1) actions, (2) container, (3) token, (4) password, (5) password_confirm, (6) text_format, or (7) markup field type, and consequently have unspecified impact, via unspecified vectors. **Reference: CVE-2016-3188**	http://cgit.drupalcode.org/prepopulate/commit/prepopulate.module?id=16cdb63cc3b256dd785e029ec17f92ddf80cc443	A-PRE-PREPO-250416/80
Not Available	08-April-16	7.5	The Prepopulate module 7.x-2.x before 7.x-2.1 for Drupal allows remote attackers to modify the REQUEST superglobal array, and consequently have unspecified impact, via a base64-encoded pp parameter. **Reference: CVE-2016-3187**	http://cgit.drupalcode.org/prepopulate/commit/prepopulate.module?id=16cdb63cc3b256dd785e029ec17f92ddf80cc443	A-PRE-PREPO-250416/81

Pulse secure

Pulse Connect Secure

Pulse Secure is a client application that connects your device to IAS's VPN.

Bypass	11-April-16	3.3	The Terminal Services Remote Desktop Protocol (RDP) client session restrictions feature in Pulse Connect Secure (aka PCS) 8.1R7 and 8.2R1 allow remote	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40166	A-PUL-PULSE-250416/82

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

			authenticated users to bypass intended access restrictions via unspecified vectors. **Reference: CVE-2016-3985**		

Puppetlabs

Puppet Enterprise

Puppet Enterprise is the leading platform for automatically delivering, operating and securing your infrastructure.

Bypass	11-April-16	6.5	Puppet Enterprise 2015.3 before 2015.3.1 allows remote attackers to bypass a host whitelist protection mechanism by leveraging the Puppet communications protocol. **Reference: CVE-2015-7330**	https://puppetlabs.com/security/cve/cve-2015-7330	A-PUP-PUPPE-250416/83

Qemu

Qemu

QEMU is a free and open-source hosted hypervisor that performs hardware virtualization. QEMU is a hosted virtual machine monitor: It emulates CPUs through dynamic binary translation and provides a set of device models, enabling it to run a variety of unmodified guest operating systems.

Denial of Service;Overflow;Memory Corruption	07-April-16	1.9	QEMU, when built with the Pseudo Random Number Generator (PRNG) back-end support, allows guest OS users to cause a denial of service (process crash) via an entropy request, which triggers arbitrary stack based allocation and memory corruption. **Reference: CVE-2016-2858**	http://git.qemu.org/?p=qemu.git;a=commit;h=60253ed1e6ec6d8e5ef2efe7bf755f475dce9956	A-QEM-QEMU-250416/84
Denial of Service;Overflow	11-April-16	2.1	The net_checksum_calculate function in net/checksum.c in QEMU allows guest OS users to cause a denial of service (out-of-bounds heap read and crash) via the payload length in a crafted packet. **Reference: CVE-2016-2857**	http://git.qemu.org/?p=qemu.git;a=commitdiff;h=362786f14a753d8a5256ef97d7c10ed576d6572b	A-QEM-QEMU-250416/85
Denial of Service;Overflow	11-April-16	4.3	Stack-based buffer overflow in hw/scsi/scsi-bus.c in QEMU, when built with SCSI-device emulation support, allows guest OS users with CAP_SYS_RAWIO permissions to cause a denial of service (instance crash) via an		A-QEM-QEMU-250416/86

			invalid opcode in a SCSI command descriptor block. **Reference: CVE-2015-5158**		
Denial of Service;Execute Code;Overflow	07-April-16	6.9	The (1) fw_cfg_write and (2) fw_cfg_read functions in hw/nvram/fw_cfg.c in QEMU before 2.4, when built with the Firmware Configuration device emulation support, allow guest OS users with the CAP_SYS_RAWIO privilege to cause a denial of service (out-of-bounds read or write access and process crash) or possibly execute arbitrary code via an invalid current entry value in a firmware configuration. **Reference: CVE-2016-1714**	http://git.qemu.org/?p=qemu.git;a=commit;h=60253ed1e6ec6d8e5ef2efe7bf755f475dce9956	A-QEM-QEMU-250416/87
Denial of Service;Execute Code	11-April-16	9.3	Use-after-free vulnerability in hw/ide/ahci.c in QEMU, when built with IDE AHCI Emulation support, allows guest OS users to cause a denial of service (instance crash) or possibly execute arbitrary code via an invalid AHCI Native Command Queuing (NCQ) AIO command. **Reference: CVE-2016-1568**	http://git.qemu.org/?p=qemu.git;a=commit;h=4ab0359a8ae182a7ac5c99609667273167703fab	A-QEM-QEMU-250416/88

Redhat

Cloudforms;Cloudforms Management Engine

Red Hat CloudForms manages private clouds, virtual environments, and public clouds in a single tool.

CloudForms include application lifecycle management capabilities as well as the capability to create hybrid public and private clouds from the broadest range of computing resources with unique portability.

Gain Privileges;Gain Information	11-April-16	1.9	Red Hat CloudForms 3.2 Management Engine (CFME) 5.4.4 and CloudForms 4.0 Management Engine (CFME) 5.5.0 do not properly encrypt data in the backend PostgreSQL database, which might allow local users to obtain sensitive data and consequently gain privileges by leveraging access to (1) database exports or (2)	https://bugzilla.redhat.com/show_bug.cgi?id=1283019	A-RED-CLOUD-250416/89

			log files. **Reference: CVE-2015-7502**		

Jboss Wildfly Application Server

WildFly,formerly known as JBoss AS, or simply JBoss, is an application server authored by JBoss, now developed by Red Hat. WildFly is written in Java, and implements the Java Platform, Enterprise Edition (Java EE) specification. It runs on multiple platforms.

Gain Information	01-April-16	5	Incomplete blacklist vulnerability in the servlet filter restriction mechanism in WildFly (formerly JBoss Application Server) before 10.0.0.Final on Windows allows remote attackers to read the sensitive files in the (1) WEB-INF or (2) META-INF directory via a request that contains (a) lowercase or (b) "meaningless" characters. **Reference: CVE-2016-0793**	https://bugzilla.redhat.com/show_bug.cgi?id=1305937	A-RED-JBOSS-250416/90

Openstack

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter.

Not Available	11-April-16	7.5	The TripleO Heat templates (tripleo-heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 7.0, do not properly use the configured RabbitMQ credentials, which makes it easier for remote attackers to obtain access to services in deployed overclouds by leveraging knowledge of the default credentials. **Reference: CVE-2015-5329**	https://access.redhat.com/errata/RHSA-2015:2650	A-RED-OPENS-250416/91

Rockwellautomation

Integrated Architecture Builder

Integrated Architecture Builder is a design tool from Rockwell Automation to help you create logical control systems and design industrial networks.

Execute Code	06-April-16	6.9	IAB.exe in Rockwell Automation Integrated Architecture Builder (IAB) before 9.6.0.8 and 9.7.x before 9.7.0.2 allows remote attackers to execute arbitrary code via a crafted project file. **Reference: CVE-2016-2277**	https://ics-cert.us-cert.gov/advisories/ICSA-16-056-01	A-ROC-INTEG-250416/92

Rubyonrails

Ruby On Rails

Ruby on Rails, or simply Rails, is a web application framework written in Ruby under the MIT License.

Directory Traversal	07-April-16	5	Directory traversal vulnerability in Action View in Ruby on Rails before 3.2.22.2 and 4.x before 4.1.14.2 allows remote attackers to read arbitrary files by leveraging an application's unrestricted use of the render method and providing a .. (dot dot) in a pathname. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-0752. **Reference: CVE-2016-2097**	http://weblog.rubyonrails.org/2016/2/29/Rails-4-2-5-2-4-1-14-2-3-2-22-2-have-been-released/	A-RUB-RUBY-250416/93

Samba

Samba

Samba is a free software re-implementation of the SMB/CIFS networking protocol.

Not Available	12-April-16	4.3	The MS-SAMR and MS-LSAD protocol implementations in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 mishandle DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "BADLOCK." **Reference: CVE-2016-2118**	https://www.samba.org/samba/security/CVE-2016-2118.html	A-SAM-SAMBA-250416/94

SAP

Java As

SAP NetWeaver Application Server or SAP Web Application Server is a component of the solution which works as a web application server to SAP solutions.

Denial of Service	08-April-16	5	The Java Startup Framework (aka jstart) in SAP JAVA AS 7.4 allows remote attackers to cause a denial of service via a crafted HTTP request, aka SAP Security Note 2259547. **Reference: CVE-2016-3980**	https://erpscan.com/advisories/erpscan-16-018-sap-java-jstart-dos/	A-SAP-JAVA-250416/95

Netweaver

SAP NetWeaver is the primary technology computing platform of the software company SAP SE,

and the technical foundation for many SAP applications. It is a solution stack of SAP's technology products.

Cross Site Scripting	07-April-16	4.3	Cross-site scripting (XSS) vulnerability in SAP NetWeaver AS Java 7.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to NavigationURLTester, aka SAP Security Note 2238375. **Reference: CVE-2016-3975**	A-SAP-NETWE-250416/96
Gain Information	07-April-16	5	The chat feature in the Real-Time Collaboration (RTC) services in SAP NetWeaver Java AS 7.4 allows remote attackers to obtain sensitive user information via unspecified vectors related to WD_CHAT, aka SAP Security Note 2255990. **Reference: CVE-2016-3973**	A-SAP-NETWE-250416/97
Directory Traversal	07-April-16	5	Directory traversal vulnerability in SAP NetWeaver AS Java 7.4 allows remote attackers to read arbitrary files via directory traversal sequences in unspecified vectors related to CrashFileDownloadServlet, aka SAP Security Note 2234971. **Reference: CVE-2016-3976**	A-SAP-NETWE-250416/98
Gain Privileges;Gain Information	07-April-16	6.5	The XML Data Archiving Service (XML DAS) in SAP NetWeaver AS Java does not check authorization, which allows remote authenticated users to obtain sensitive information, gain privileges, or possibly have unspecified other impact via requests to (1) webcontent/cas/cas_enter.jsp, (2) webcontent/cas/cas_validate.jsp, or (3) webcontent/aas/aas_store.jsp, aka SAP Security Note 1945215.	A-SAP-NETWE-250416/99

			Reference: CVE-2015-8840		
Denial of Service	07-April-16	7.5	XML external entity (XXE) vulnerability in the Configuration Wizard in SAP NetWeaver Java AS 7.4 allows remote attackers to cause a denial of service, conduct SMB Relay attacks, or access arbitrary files via a crafted XML request, related to the ctcprotocol servlet, aka SAP Security Note 2235994. **Reference: CVE-2016-3974**		A-SAP-NETWE-250416/100

Sharp

Eva Animater

Extended Vector Animation (EVA) is a web-based vector graphic file format developed by Sharp Corporation in 1996.

Execute Code; Overflow	05-April-16	6.8	Buffer overflow in the ActiveX control in Sharp EVA Animeter allows remote attackers to execute arbitrary code via a crafted web page. **Reference: CVE-2016-1176**		A-SHA-EVA A-250416/101

Spip

Spip

SPIP is a free software content management system designed for web site publishing, oriented towards online collaborative editing.

Execute Code	08-April-16	7.5	The encoder_contexte_ajax function in ecrire/inc/filtres.php in SPIP 2.x before 2.1.19, 3.0.x before 3.0.22, and 3.1.x before 3.1.1 allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via a crafted serialized object. **Reference: CVE-2016-3154**	https://blog.spip.net/Mise-a-jour-CRITIQUE-de-securite-Sortie-de-SPIP-3-1-1-SPIP-3-0-22-et-SPIP-2-1.html?lang=fr	A-SPI-SPIP-250416/102

Squid-cache

Squid

Squid is a caching and forwarding web proxy. It has a wide variety of uses, from speeding up a web server by caching repeated requests; to caching web and DNS.

Denial of Service;Overflow	07-April-16	5	Squid 3.x before 3.5.16 and 4.x before 4.0.8 improperly perform bounds checking, which allows remote attackers to cause a	http://www.squid-cache.org/Versions/v3/3.5/changesets/squid-3.5-	A-SQU-SQUID-250416/103

			denial of service via a crafted HTTP response, related to Vary headers. **Reference: CVE-2016-3948**	14016.patch	
Denial of Service;Overflow	07-April-16	7.5	Heap-based buffer overflow in the Icmp6::Recv function in icmp/Icmp6.cc in the pinger in Squid before 3.5.16 and 4.x before 4.0.8 allows remote servers to cause a denial of service (performance degradation or transition failures) or write sensitive information to log files via an ICMPv6 packet. **Reference: CVE-2016-3947**	http://www.squid-cache.org/Advisories/SQUID-2016_3.txt	A-SQU-SQUID-250416/104

Trend Micro

Password Manager

A password manager is a software application that helps a user store and organize passwords.

Execute Code	11-April-16	10	The HTTP server in Trend Micro Password Manager allows remote web servers to execute arbitrary commands via the url parameter to (1) api/openUrlInDefaultBrowser or (2) api/showSB. **Reference: CVE-2016-3987**	http://blog.trendmicro.com/information-on-reported-vulnerabilities-in-trend-micro-password-manager/	A-TRE-PASSW-250416/105

Xmlsoft

Libxml2

libxml2 is a software library for parsing XML documents. It is also the basis for the libxslt library which processes XSLT-1.0 stylesheets.

Denial of Service;Overflow	13-April-16	5	dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the "<!DOCTYPE html" substring in a crafted HTML document. **Reference: CVE-2015-8806**		A-XML-LIBXM-250416/106

Zimbra

Zimbra Collaboration Server

Zimbra Collaboration is an open, secure collaboration server for email, calendaring, file sharing, tasks and more.

Cross-site	08-April-	6.8	Multiple cross-site request	https://wiki.zimbr	A-ZIM-

Request Forgery	16		forgery (CSRF) vulnerabilities in the Mail interface in Zimbra Collaboration Server (ZCS) before 8.5 allow remote attackers to hijack the authentication of arbitrary users for requests that change account preferences via a SOAP request to service/soap/BatchRequest. **Reference: CVE-2015-6541**	a.com/wiki/Security/Collab/86#Notes_from_8.5_.28Jetty.29	ZIMBR-250416/107

Beanshell Project/Debian

Beanshell/Debian Linux

BeanShell is a Java-like scripting language, invented by Patrick Niemeyer. It runs in the Java Runtime Environment (JRE) and uses a variation of the Java.
Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.

Execute Code	07-April-16	6.8	BeanShell (bsh) before 2.0b6, when included on the classpath by an application that uses Java serialization or XStream, allows remote attackers to execute arbitrary code via crafted serialized data, related to XThis.Handler. **Reference: CVE-2016-2510**	https://github.com/beanshell/beanshell/commit/7c68fde2d6fc65e362f20863d868c112a90a9b49	A-BEA-BEANS-250416/108

Erlang/Novell

OTP/Opensuse

OTP is a collection of useful middleware, libraries and tools written in Erlang programming language.
openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.

Gain Information	07-April-16	4.3	Erlang/OTP before 18.0-rc1 does not properly check CBC padding bytes when terminating connections, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, a variant of CVE-2014-3566 (aka POODLE). **Reference: CVE-2015-2774**	https://web.archive.org/web/20150905124006/http://www.erlang.org/news/85	A-ERL-OTP/O-250416/109

Hardware(H)

Siemens

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

Scalance S613

Security Module for the protection of automation devices and automation networks and to safeguard industrial communication.

Denial of Service	08-April-16	5	Siemens SCALANCE S613 allows remote attackers to cause a denial of service (web-server outage) via traffic to TCP port 443. **Reference: CVE-2016-3963**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-751155.pdf	H-SIE-SCALA-250416/110

Operating System (OS)

Cisco

IOS

iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.

Gain Information	13-April-16	5	Cisco IOS before 15.2(2)E1 on Catalyst switches allows remote attackers to obtain potentially sensitive software-version information via a request to the Network Mobility Services Protocol (NMSP) port, aka Bug ID CSCum62591. **Reference: CVE-2016-1378**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160413-nms	OS-CIS-IOS-250416/111

Ios Xr

IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS).

Denial of Service	12-April-16	5	Cisco IOS XR 4.2.3, 4.3.0, 4.3.4, and 5.3.1 on ASR 9000 devices allows remote attackers to cause a denial of service (CRC and symbol errors, and interface flap) via crafted bit patterns in packets, aka Bug ID CSCuv78548. **Reference: CVE-2016-1376**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160412-asr	OS-CIS-IOS X-250416/112

Fortinet

Fortios

FortiOS 5.0, the world's most powerful security operating system, is the foundation for all Fortinet FortiGate integrated security platforms.

Cross Site Scripting	08-April-16	4.3	The Web User Interface (WebUI) in FortiOS 5.0.x before 5.0.13, 5.2.x before 5.2.3, and 5.4.x before 5.4.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks or cross-site scripting (XSS) attacks via the	http://www.fortiguard.com/advisory/fortios-open-redirect-vulnerability	OS-FOR-FORTI-250416/113

			"redirect" parameter to "login." **Reference: CVE-2016-3978**		

Huawei

E3276s Firmware

Huawei E3276 is an 4g LET Modem which provides upto 150mbps of high speed. It also supports 3g and 2g networks.

Not Available	11-April-16	5.8	Huawei E3276s USB modems with software before E3276s-150TCPU-V200R002B436D09SP00C00 allow man-in-the-middle attackers to intercept, spoof, or modify network traffic via unspecified vectors related to a fake network. **Reference: CVE-2016-3676**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160330-01-dongle-en	OS-HUA-E3276-250416/114

Microsoft

Windows 10

Windows 10 is a personal computer operating system developed and released by Microsoft as part of the Windows NT family of operating systems.

	12-April-16	7.2	The Secondary Logon Service in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Secondary Logon Elevation of Privilege Vulnerability." **Reference: CVE-2016-0135**	http://technet.microsoft.com/en-us/security/bulletin/ms16-046	OS-MIC-WINDO-250416/115

Netapp

Clustered Data Ontap

NetApp clustered Data ONTAP software is the foundation of the Data Fabric, vision for the future of data management.

Gain Information	07-April-16	5.8	NetApp Clustered Data ONTAP 8.3.1 does not properly verify X.509 certificates from TLS servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **Reference: CVE-2016-1563**	https://kb.netapp.com/support/index?page=content&id=9010064	OS-NET-CLUST-250416/115

Novell

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. It is widely used throughout

the world, particularly in Germany. The focus of its development is creating usable open-source tools for software developers and system administrators, while providing a user-friendly desktop, and feature-rich server environment.

Execute Code	13-April-16	10	Multiple unspecified vulnerabilities in the obs-service-extract_file package before 0.3-5.1 in openSUSE Leap 42.1 and before 0.3-3.1 in openSUSE 13.2 allow attackers to execute arbitrary commands via a service definition, related to executing unzip with "illegal options." **Reference: CVE-2016-4007**	https://build.opensuse.org/request/show/361096	OS-NOV-LEAP;-250416/116

Paloaltonetworks

Pan-os

Panos is a discontinued computer operating system developed by Acorn Computers in the 1980s, which ran on the 32016 Second Processor for the BBC Micro and the Acorn Cambridge Workstation.

Denial of Service;Overflow	12-April-16	5	The GlobalProtect Portal in Palo Alto Networks PAN-OS before 5.0.18, 6.0.x before 6.0.13, 6.1.x before 6.1.10, and 7.0.x before 7.0.5H2 allows remote attackers to cause a denial of service (service crash) via a crafted request. **Reference: CVE-2016-3656**	http://securityadvisories.paloaltonetworks.com/Home/Detail/37	OS-PAL-PAN-O-250416/117
Denial of Service;Execute Code;Overflow	12-April-16	10	Buffer overflow in the GlobalProtect Portal in Palo Alto Networks PAN-OS before 5.0.18, 6.0.x before 6.0.13, 6.1.x before 6.1.10, and 7.0.x before 7.0.5 allows remote attackers to cause a denial of service (device crash) or possibly execute arbitrary code via an SSL VPN request. **Reference: CVE-2016-3657**	http://securityadvisories.paloaltonetworks.com/Home/Detail/38	OS-PAL-PAN-O-250416/118
Execute Code	12-April-16	10	The management web interface in Palo Alto Networks PAN-OS before 5.0.18, 6.0.x before 6.0.13, 6.1.x before 6.1.10, and 7.0.x before 7.0.5 allows remote attackers to execute arbitrary OS commands via an	http://securityadvisories.paloaltonetworks.com/Home/Detail/36	OS-PAL-PAN-O-250416/119

			unspecified API call. **Reference: CVE-2016-3655**		

Sharp

Aquos Hn-pp150 Firmware

Aquos HN-PP150, a photo printer that can also be used to display images on a TV via its HDMI output.

Cross-site Request Forgery	05-April-16	5.8	Cross-site request forgery (CSRF) vulnerability in AQUOS Photo Player HN-PP150 1.02.00.04 through 1.03.01.04 allows remote attackers to hijack the authentication of arbitrary users. **Reference: CVE-2016-1175**	http://www.sharp.co.jp/support/photoplayer/fw_update.html	OS-SHA-AQUOS-250416/120

Sophos

Cyberoam Cr100ing Utm Firmware;Cyberoam Cr35ing Utm Firmware

Cyberoam NG series of Unified Threat Management appliances are the Next-Generation network security appliances that include UTM security features and performance required for future networks. The NG series for SOHO offer “the fastest UTMs made for SMBs” to small offices.

Cross Site Scripting	06-April-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Sophos Cyberoam CR100iNG UTM appliance with firmware 10.6.3 MR-1 build 503, CR35iNG UTM appliance with firmware 10.6.2 MR-1 build 383, and CR35iNG UTM appliance with firmware 10.6.2 Build 378 allow remote attackers to inject arbitrary web script or HTML via the (1) ipFamily parameter to corporate/webpages/trafficdiscovery/LiveConnections.jsp; the (2) ipFamily, (3) applicationname, or (4) username parameter to corporate/webpages/trafficdiscovery/LiveConnectionDetail.jsp; or the (5) X-Forwarded-For HTTP header. **Reference: CVE-2016-3968**		OS-SOP-CYBER-250416/121

Operating System/Application(OS/A)

Debian/Debian;Python

Debian Linux/Python-imaging/Pillow

Debian is a Unix-like computer operating system that is composed entirely of free software, most

of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.
The Python Imaging Library (PIL) adds image processing capabilities to your Python interpreter. Python Imaging Library (abbreviated as PIL) is a free library for the Python programming.

Denial of Service;Overflow	13-April-16	4.3	Buffer overflow in the ImagingPcdDecode function in PcdDecode.c in Pillow before 3.1.1 and Python Imaging Library (PIL) 1.1.7 and earlier allows remote attackers to cause a denial of service (crash) via a crafted PhotoCD file. **Reference: CVE-2016-2533**	https://github.com/python-pillow/Pillow/blob/c3cb690fed5d4bf0c45576759de55d054916c165/CHANGES.rst	OS-A-DEB-DEBIA-250416/122

Debian/Dhcpcd Project

Debian Linux/Dhcpcd

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.
dhcpcd is a DHCP and DHCPv6 client. It is currently the most feature-rich open source DHCP client

Denial of Service;Overflow	11-April-16	5	The decode_search function in dhcp.c in dhcpcd 3.x does not properly free allocated memory, which allows remote DHCP servers to cause a denial of service via a crafted response. **Reference: CVE-2012-6700**	https://bugs.launchpad.net/ubuntu/+source/dhcpcd/+bug/1517226	OS-A-DEB-DEBIA-250416/123
Denial of Service;Overflow	11-April-16	5	The decode_search function in dhcp.c in dhcpcd 3.x allows remote DHCP servers to cause a denial of service (out-of-bounds read) via a crafted response. **Reference: CVE-2012-6699**	https://bugs.launchpad.net/ubuntu/+source/dhcpcd/+bug/1517226	OS-A-DEB-DEBIA-250416/124
Denial of Service;Overflow	11-April-16	5	The decode_search function in dhcp.c in dhcpcd 3.x allows remote DHCP servers to cause a denial of service (out-of-bounds write) via a crafted response. **Reference: CVE-2012-6698**	https://bugs.launchpad.net/ubuntu/+source/dhcpcd/+bug/1517226	OS-A-DEB-DEBIA-250416/125

Debian/Drupal

Debian Linux/Drupal

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known

as the Debian Project.
Drupal is content management software. It's used to make many of the websites and applications you use every day

Http R.Spl.	12-April-16	4.3	CRLF injection vulnerability in the drupal_set_header function in Drupal 6.x before 6.38, when used with PHP before 5.1.2, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by leveraging a module that allows user-submitted data to appear in HTTP headers. **Reference: CVE-2016-3166**	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/126
Gain Information	12-April-16	5	The "have you forgotten your password" links in the User module in Drupal 7.x before 7.43 and 8.x before 8.0.4 allow remote attackers to obtain sensitive username information by leveraging a configuration that permits using an email address to login and a module that permits logging in. **Reference: CVE-2016-3170**	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/127
Not Available	12-April-16	5	The XML-RPC system in Drupal 6.x before 6.38 and 7.x before 7.43 might make it easier for remote attackers to conduct brute-force attacks via a large number of calls made at once to the same method. **Reference: CVE-2016-3163**	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/128
Not Available	12-April-16	5.8	Drupal 6.x before 6.38, 7.x before 7.43, and 8.x before 8.0.4 might allow remote attackers to conduct open redirect attacks by leveraging (1) custom code or (2) a form shown on a 404 error page, related to path manipulation. **Reference: CVE-2016-3164**	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/129
Not Available	12-April-16	6.4	Open redirect vulnerability in the drupal_goto function in Drupal 6.x before 6.38, when	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/13

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

			used with PHP before 5.4.7, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a double-encoded URL in the "destination" parameter. **Reference: CVE-2016-3167**		0
Gain Privileges	12-April-16	6.8	The User module in Drupal 6.x before 6.38 and 7.x before 7.43 allows remote attackers to gain privileges by leveraging contributed or custom code that calls the user_save function with an explicit category and loads all roles into the array. **Reference: CVE-2016-3169**	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/131
Execute Code	12-April-16	6.8	Drupal 6.x before 6.38, when used with PHP before 5.4.45, 5.5.x before 5.5.29, or 5.6.x before 5.6.13, might allow remote attackers to execute arbitrary code via vectors related to session data truncation. **Reference: CVE-2016-3171**	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/132
Not Available	12-April-16	8.5	The System module in Drupal 6.x before 6.38 and 7.x before 7.43 might allow remote attackers to hijack the authentication of site administrators for requests that download and run files with arbitrary JSON-encoded content, aka a "reflected file download vulnerability." **Reference: CVE-2016-3168**	https://www.drupal.org/SA-CORE-2016-001	OS-A-DEB-DEBIA-250416/133

Debian/Kamailio

Debian Linux/Kamailio

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.

Kamailio (successor of former OpenSER and SER) is an Open Source SIP Server released under GPL, able to handle thousands of call setups per second. Kamailio can be used to build large platforms for VoIP and realtime communications – presence, WebRTC, Instant messaging and

other applications.

Denial of Service;Execute Code;Overflow;Memory Corruption	11-April-16	10	Heap-based buffer overflow in the encode_msg function in encode_msg.c in the SEAS module in Kamailio (formerly OpenSER and SER) before 4.3.5 allows remote attackers to cause a denial of service (memory corruption and process crash) or possibly execute arbitrary code via a large SIP packet. **Reference: CVE-2016-2385**	http://www.kamailio.org/pub/kamailio/4.3.5/ChangeLog	OS-A-DEB-DEBIA-250416/134

Debian/Oar Project

Debian Linux/OAR

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.

OAR is a resource manager (or batch scheduler) for large clusters.

Gain Privileges;Gain Information	11-April-16	9	The oarsh script in OAR before 2.5.7 allows remote authenticated users of a cluster to obtain sensitive information and possibly gain privileges via vectors related to OpenSSH options. **Reference: CVE-2016-1235**	http://oar.imag.fr/oar_2.5.7	OS-A-DEB-DEBIA-250416/135

Debian/Optipng

Debian Linux/Optipng

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project

A PNG optimizer that recompresses the image files to a smaller size.

Denial of Service;Overflow	13-April-16	4.3	The bmp_read_rows function in pngxtern/pngxrbmp.c in OptiPNG before 0.7.6 allows remote attackers to cause a denial of service (invalid memory write and crash) via a series of delta escapes in a crafted BMP image. **Reference: CVE-2016-2191**	https://sourceforge.net/p/optipng/bugs/59/	OS-A-DEB-DEBIA-250416/136
Denial of Service;Execute Code;Overfl	13-April-16	9.3	Heap-based buffer overflow in the bmp_read_rows function in pngxrbmp.c in OptiPNG before 0.7.6 allows remote attackers to	https://sourceforge.net/p/optipng/bugs/56/	OS-A-DEB-DEBIA-250416/137

ow			cause a denial of service (out-of-bounds read or write access and crash) or possibly execute arbitrary code via a crafted image file. **Reference: CVE-2016-3981**		

Debian/Python

Debian Linux/ Python

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.

Python Imaging Library (abbreviated as PIL) is a free library for the Python programming.

Denial of Service;Overflow	13-April-16	4.3	Buffer overflow in the ImagingFliDecode function in libImaging/FliDecode.c in Pillow before 3.1.1 allows remote attackers to cause a denial of service (crash) via a crafted FLI file. **Reference: CVE-2016-0775**	https://github.com/python-pillow/Pillow/commit/893a40850c2d5da41537958e40569c029a6e127b	OS-A-DEB-DEBIA-250416/138
Overflow	13-April-16	4.3	Buffer overflow in the ImagingLibTiffDecode function in libImaging/TiffDecode.c in Pillow before 3.1.1 allows remote attackers to overwrite memory via a crafted TIFF file. **Reference: CVE-2016-0740**	https://github.com/python-pillow/Pillow/blob/c3cb690fed5d4bf0c45576759de55d054916c165/CHANGES.rst	OS-A-DEB-DEBIA-250416/139

Debian/Rubyonrails

Debian Linux/Ruby On Rails

Ruby on Rails, or simply Rails, is a web application framework written in Ruby under the MIT License.

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.

Execute Code	07-April-16	7.5	Action Pack in Ruby on Rails before 3.2.22.2, 4.x before 4.1.14.2, and 4.2.x before 4.2.5.2 allows remote attackers to execute arbitrary Ruby code by leveraging an application's unrestricted use of the render method. **Reference: CVE-2016-2098**	http://weblog.rubyonrails.org/2016/2/29/Rails-4-2-5-2-4-1-14-2-3-2-22-2-have-been-released/	OS-A-DEB-DEBIA-250416/140

Debian/Spip

Debian Linux/Spip

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.
SPIP is a free software content management system designed for web site publishing, oriented towards online collaborative editing

Execute Code	08-April-16	7.5	SPIP 2.x before 2.1.19, 3.0.x before 3.0.22, and 3.1.x before 3.1.1 allows remote attackers to execute arbitrary PHP code by adding content, related to the filtrer_entites function. **Reference: CVE-2016-3153**	https://blog.spip.net/Mise-a-jour-CRITIQUE-de-securite-Sortie-de-SPIP-3-1-1-SPIP-3-0-22-et-SPIP-2-1.html?lang=fr	OS-A-DEB-DEBIA-250416/141

Debian/Websvn

Debian Linux/Websvn

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project. Three main branches are offered: Stable, Testing and Unstable.
WebSVN is a PHP-based client that, together with Apache, gives you a web-browser view of your Subversion repository

Cross Site Scripting	07-April-16	4.3	Cross-site scripting (XSS) vulnerability in WebSVN 2.3.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the path parameter to log.php. **Reference: CVE-2016-2511**		OS-A-DEB-DEBIA-250416/142

Debian/Xmlsoft

Debian Linux/Libxml2

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project.
libxml2 is a software library for parsing XML documents.

Denial of Service; Overflow; Gain Information	11-April-16	7.5	The htmlParseComment function in HTMLparser.c in libxml2 allows attackers to obtain sensitive information, cause a denial of service (out-of-bounds heap memory access and application crash), or possibly have unspecified other impact via an unclosed HTML comment. **Reference: CVE-2015-8710**	https://bugzilla.gnome.org/show_bug.cgi?id=746048	OS-A-DEB-DEBIA-250416/143

Debian/Xymon

Debian Linux/Xymon

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian Project

Xymon is a system for monitoring of hosts and networks, inspired by the Big Brother system

Not Available	13-April-16	2.1	lib/xymond_ipc.c in Xymon 4.1.x, 4.2.x, and 4.3.x before 4.3.25 use weak permissions (666) for an unspecified IPC message queue, which allows local users to inject arbitrary messages by writing to that queue. **Reference: CVE-2016-2057**	https://sourceforge.net/p/xymon/code/7891/	OS-A-DEB-DEBIA-250416/144
Cross Site Scripting	13-April-16	3.5	Multiple cross-site scripting (XSS) vulnerabilities in Xymon 4.1.x, 4.2.x, and 4.3.x before 4.3.25 allow (1) remote Xymon clients to inject arbitrary web script or HTML via a status-message, which is not properly handled in the "detailed status" page, or (2) remote authenticated users to inject arbitrary web script or HTML via an acknowledgement message, which is not properly handled in the "status" page. **Reference: CVE-2016-2058**	https://sourceforge.net/p/xymon/code/7892/	OS-A-DEB-DEBIA-250416/145
Gain Information	13-April-16	5	xymond/xymond.c in xymond in Xymon 4.1.x, 4.2.x, and 4.3.x before 4.3.25 allow remote attackers to read arbitrary files in the configuration directory via a "config" command. **Reference: CVE-2016-2055**	https://sourceforge.net/p/xymon/code/7890/	OS-A-DEB-DEBIA-250416/146
Execute Code	13-April-16	6.5	xymond in Xymon 4.1.x, 4.2.x, and 4.3.x before 4.3.25 allow remote authenticated users to execute arbitrary commands via shell metacharacters in the adduser_name argument in (1) web/useradm.c or (2) web/chpasswd.c. **Reference: CVE-2016-2056**	https://sourceforge.net/p/xymon/code/7892/	OS-A-DEB-DEBIA-250416/147
Denial of	13-April-	7.5	Multiple buffer overflows in	https://sourcefor	OS-A-DEB-

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	16		xymond/xymond.c in xymond in Xymon 4.1.x, 4.2.x, and 4.3.x before 4.3.25 allow remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a long filename, involving handling a "config" command. **Reference: CVE-2016-2054**	ge.net/p/xymon/code/7860/	DEBIA-250416/148

Fedoraproject/Nodejs

Fedora/Node.js

A Linux based operating system.
Node.js is an open-source, cross-platform runtime environment for developing server-side Web applications.

Http R.Spl.; Bypass	07-April-16	4.3	The HTTP header parsing code in Node.js 0.10.x before 0.10.42, 0.11.6 through 0.11.16, 0.12.x before 0.12.10, 4.x before 4.3.0, and 5.x before 5.6.0 allows remote attackers to bypass an HTTP response-splitting protection mechanism via UTF-8 encoded Unicode characters in the HTTP header, as demonstrated by %c4%8d %c4%8a. **Reference: CVE-2016-2216**	https://nodejs.org/en/blog/vulnerability/february-2016-security-releases/	OS-A-FED-FEDOR-250416/149
Not Available	07-April-16	5	Node.js 0.10.x before 0.10.42, 0.12.x before 0.12.10, 4.x before 4.3.0, and 5.x before 5.6.0 allow remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header. **Reference: CVE-2016-2086**	https://nodejs.org/en/blog/vulnerability/february-2016-security-releases/	OS-A-FED-FEDOR-250416/150

Fedoraproject/Proftpd

Fedora/Proftpd

Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project.
ProFTPD is Free and open-source software, compatible with Unix-like systems and Microsoft Windows (via Cygwin).

Not Available	05-April-16	10	The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a	http://bugs.proftpd.org/show_bug.cgi?id=4230	OS-A-FED-FEDOR-250416/151

weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.
Reference: CVE-2016-3125

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