National Critical Information Infrastructure Protection Centre

CVE Report

15- 29 April 2016

Vol. 3 No.7

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Application					
Allround Automations					
Pl/sql Developer PL/SQL Developer is an Integrated Development Environment that is specifically targeted at the development of stored program units for Oracle Databases.					
Execute Code	25-April-16	6.8	Allround Automations PL/SQL Developer 11 before 11.0.6 relies on unverified HTTP data for updates, which allows man-in-the-middle attackers to execute arbitrary code by modifying fields in the client-server data stream. **Reference:CVE-2016-2346**	NA	A-ALL-PL/SQ-30516/1
Apache					
Hadoop Hadoop is an open-source framework that allows to store and process big data in a distributed environment across clusters of computers using simple programming models.					
Gain Information	19-April-2016	2.1	Apache Hadoop 2.6.x encrypts intermediate data generated by a MapReduce job and stores it along with the encryption key in a credentials file on disk when the Intermediate data encryption feature is enabled, which allows local users to obtain sensitive information by reading the file. **Reference : CVE-2015-1776**	http://mail-archives.apache.org/mod_mbox/hadoop-general/201602.mbox/%3CCAGCyb56CPgQMcxZ7jP87SfM5OKGx+E49DtrzCTQ6+nQf2a4nSA@mail.gmail.com%3E	A-APA-HADOO-30516/2

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

National Critical Information Infrastructure Protection Centre

CVE Report

15- 29 April 2016 **Vol. 3 No.7**

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Blackberry					
Enterprise Server An enterprise server is a computer server that includes programs required to collectively serve the requirements of an enterprise instead of an individual user, unit or specific application.					
Cross Site Scripting	22-April-2016	4.3	Cross-site scripting (XSS) vulnerability in the Management Console in BlackBerry Enterprise Server (BES) 12 before 12.4.1 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-3126**	http://www.blackberry.com/btsc/KB38119	A-BLA-ENTER-30516/3
Cross Site Scripting	22-April-2016	4.3	Cross-site scripting (XSS) vulnerability in the Management Console in BlackBerry Enterprise Server (BES) 12 before 12.4.1 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, a different vulnerability . **Reference :CVE-2016-1917.**	http://www.blackberry.com/btsc/KB38118	A-BLA-ENTER-30516/4
Cross Site Scripting	22-April-2016	4.3	Cross-site scripting (XSS) vulnerability in the Management Console in BlackBerry Enterprise Server (BES) 12 before 12.4.1 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, a different vulnerability. **Reference :CVE-2016-1918.**	http://www.blackberry.com/btsc/KB38118	A-BLA-ENTER-30516/5

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	22-April-2016	3.5	Cross-site scripting (XSS) vulnerability in the Management Console in BlackBerry Enterprise Server (BES) 12 before 12.4.1 allows remote authenticated users to inject arbitrary web script or HTML by leveraging basic administrative access to create a crafted policy, leading to improper rendering on a certain Export IT screen. **Reference** :**CVE-2016-1916**	http://www.blackberry.com/btsc/KB38117	A-BLA-ENTER-30516/6
Cisco					
Adaptive Security Appliance Software Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.					
Denial of Service	21-April-2016	7.8	The DHCPv6 relay implementation in Cisco Adaptive Security Appliance (ASA) Software 9.4.1 allows remote attackers to cause a denial of service (device reload) via crafted DHCPv6 packets, aka Bug ID CSCus23248. **Reference** :**CVE-2016-1367**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-asa-dhcpv6	A-CIS-ADAPT-30516/7
Dotcms					
Dotcms DotCMS is a free software / open source web content management system (WCM) for building/managing websites, content and content driven web applications.					
Dir. Trav.	18-April-2016	4	Directory traversal vulnerability in the	http://dotcms.com/security	A-DOT-DOTCM-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			dotTailLogServlet in dotCMS before 3.5.1 allows remote authenticated administrators to read arbitrary files via a .. (dot dot) in the fileName parameter. **Reference** : **CVE-2016-3972**	/SI-34	30516/8
Execute Code; Sql Injection	19-April-2016	6.5	SQL injection vulnerability in the Workflow Screen in dotCMS before 3.3.2 allows remote administrators to execute arbitrary SQL commands via the orderby parameter. **Reference** :**CVE-2016-4040**	http://dotcms.com/security/SI-36	A-DOT-DOTCM-30516/9
Execute Code Sql Injection Gain Information	19-April-2016	4	SQL injection vulnerability in dotCMS before 3.5 allows remote administrators to execute arbitrary SQL commands via the c0-e3 parameter to dwr/call/plaincall/UserAjax.getUsersList.dwr. **Reference** :**CVE-2016-3688**	http://dotcms.com/security/SI-32	A-DOT-DOTCM-30516/ 10
Cross Site Scripting	18-April-2016	3.5	Cross-site scripting (XSS) vulnerability in lucene_search.jsp in dotCMS before 3.5.1 allows remote authenticated administrators to inject arbitrary web script or	http://dotcms.com/security/SI-33	A-DOT-DOTCM-30516/11

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			HTML via the query parameter to c/portal/layout. **Reference** :**CVE-2016-3971**		
Ecava					
Integraxor IntegraXor is a suite of tools used to create and run a web-based human-machine interface for a SCADA system.					
Gain Information	21-April-2016	7.8	The HMI web server in Ecava IntegraXor before 5.0 build 4522 allows remote attackers to obtain sensitive cleartext information by sniffing the network. **Reference** :**CVE-2016-2306**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/12
Gain Information	21-April-2016	4.3	Ecava IntegraXor before 5.0 build 4522 does not include the HTTPOnly flag in a Set-Cookie header for the session cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie. **Reference** : **CVE-2016-2304**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/13
Gain Information	21-April-2016	5	Ecava IntegraXor before 5.0 build 4522 allows remote attackers to obtain sensitive information by reading detailed error messages. **Reference** :**CVE-2016-2302**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/14

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Bypass	21-April-2016	6.4	Ecava IntegraXor before 5.0 build 4522 allows remote attackers to bypass authentication and access unspecified web pages via unknown vectors. **Reference :CVE-2016-2300**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/15
Execute Code; Sql Injection	21-April-2016	6.5	SQL injection vulnerability in Ecava IntegraXor before 5.0 build 4522 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference :CVE-2016-2301**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/16
Execute Code; Sql Injection	21-April-2016	7.5	SQL injection vulnerability in Ecava IntegraXor before 5.0 build 4522 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **Reference : CVE-2016-2299**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/17
Http R.Spl.	21-April-2016	5	CRLF injection vulnerability in Ecava IntegraXor before 5.0 build 4522 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a crafted URL. **Reference :CVE-2016-**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/18

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
			2303		
Cross Site Scripting	21-April-2016	4.3	Cross-site scripting (XSS) vulnerability in Ecava IntegraXor before 5.0 build 4522 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference** :**CVE-2016-2305**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03	A-ECA-INTEG-30516/19
EMC					
Vipr Srm EMC ViPR SRM is storage resource management software that enables IT to visualize storage relationships, analyze configurations and capacity growth, and optimize resources to improve return on investment (ROI) in traditional and software-defined storage environments.					
Cross-site Request Forgery	20-April-2016	6.8	Multiple cross-site request forgery (CSRF) vulnerabilities in administrative pages in EMC ViPR SRM before 3.7 allow remote attackers to hijack the authentication of administrators. **Reference** :**CVE-2016-0891**	http://seclists.org/bugtraq/2016/Apr/106	A-EMC-VIPR-30516/20
Foxitsoftware					
Phantompdf;Reader Foxit PhantomPDF is a PDF creator, editor and reader					
Denial of Service	22-April-2016	4.3	Foxit Reader and PhantomPDF before 7.3.4 on Windows improperly report format errors recursively, which allows remote attackers to cause a denial of service (application hang) via a crafted PDF.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-30516/21

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service	22-April-2016	5	**Reference** :**CVE-2016-4062** Foxit Reader and PhantomPDF before 7.3.4 on Windows allow remote attackers to cause a denial of service (application crash) via a crafted content stream.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-30516/22
Denial of Service	22-April-2016	5	**Reference** :**CVE-2016-4061** Use-after-free vulnerability in Foxit Reader and PhantomPDF before 7.3.4 on Windows allows remote attackers to cause a denial of service (application crash) via unspecified vectors.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-30516/23
Denail of Service Overflow	22-April-2016	6.8	**Reference** :**CVE-2016-4060** The ConvertToPDF plugin in Foxit Reader and PhantomPDF before 7.3.4 on Windows, when the gflags app is enabled, allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted (1) JPEG, (2) GIF, or (3) BMP image.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-30516/24
Execute Code	22-April-2016	6.8	**Reference** :**CVE-2016-4065** Use-after-free vulnerability in the XFA forms handling functionality in Foxit	https://www.foxitsoftware.com/support/security-	A-FOX-PHANT-30516/25

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reader and PhantomPDF before 7.3.4 on Windows allows remote attackers to execute arbitrary code via a crafted remerge call. **Reference :CVE-2016-4064**	bulletins.php	
Execute Code	22-April-2016	6.8	Use-after-free vulnerability in Foxit Reader and PhantomPDF before 7.3.4 on Windows allows remote attackers to execute arbitrary code via an object with a revision number of -1 in a PDF document. **Reference :CVE-2016-4063**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-30516/26
Execute Code	22-April-2016	6.8	Use-after-free vulnerability in Foxit Reader and PhantomPDF before 7.3.4 on Windows allows remote attackers to execute arbitrary code via a crafted FlateDecode stream in a PDF document. **Reference :CVE-2016-4059**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHANT-30516/27
Google					
Chrome Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.					
Bypass	18-April-2016	5	The download implementation in Google Chrome before 50.0.2661.75 on Android allows remote attackers	https://crbug.com/570750	A-GOO-CHROM-30516/28

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			to bypass intended pathname restrictions via unspecified vectors. **Reference** :**CVE-2016-1656**		
Bypass;Gain Information	18-April-2016	4.3	The Extensions subsystem in Google Chrome before 50.0.2661.75 incorrectly relies on GetOrigin method calls for origin comparisons, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted extension. **Reference** :**CVE-2016-1658**	https://crbug.com/573317	A-GOO-CHROM-30516/29
Denial of Service	18-April-2016	10	Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference** :**CVE-2016-1659**	https://crbug.com/602697	A-GOO-CHROM-30516/30
Denial of Service	18-April-2016	6.8	Google Chrome before 50.0.2661.75 does not properly consider that frame removal may occur during callback execution, which allows remote attackers to cause a denial of service (use-after-free) or possibly have	https://crbug.com/582008	A-GOO-CHROM-30516/31

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			unspecified other impact via a crafted extension. **Reference :CVE-2016-1655**		
Denial of Service	18-April-2016	4.3	The media subsystem in Google Chrome before 50.0.2661.75 does not initialize an unspecified data structure, which allows remote attackers to cause a denial of service (invalid read operation) via unknown vectors. **Reference :CVE-2016-1654**	http://googlechromereleases.blogspot.com/2016/04/stable-channel-update_13.html	A-GOO-CHROM-30516/32
Denial of Service;Gain Information	18-April-2016	5.8	fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 50.0.2661.75, does not properly implement the sycc420_to_rgb and sycc422_to_rgb functions, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via crafted JPEG 2000 data in a PDF document. **Reference :CVE-2016-1651**	https://crbug.com/591785	A-GOO-CHROM-30516/33
Denail of Service Overflow	18-April-2016	9.3	The LoadBuffer implementation in Google V8, as used in Google Chrome before 50.0.2661.75,	http://googlechromereleases.blogspot.com/2016/04/stable-	A-GOO-CHROM-30516/34

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			mishandles data types, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc. **Reference :CVE-2016-1653**	channel-update_13.html	
Cross Site Scripting	18-April-2016	4.3	Cross-site scripting (XSS) vulnerability in the ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the Extensions subsystem in Google Chrome before 50.0.2661.75 allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)." **Reference :CVE-2016-1652**	http://googlechromereleases.blogspot.com/2016/04/stable-channel-update_13.html	A-GOO-CHROM-30516/35
NA	18-April-2016	4.3	The WebContentsImpl::FocusLocationBarByDefault function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 50.0.2661.75 mishandles focus for	http://googlechromereleases.blogspot.com/2016/04/stable-channel-update_13.html	A-GOO-CHROM-30516/36

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			certain about:blank pages, which allows remote attackers to spoof the address bar via a crafted URL. **Reference** : **CVE-2016-1657**		
HP					
Data Protector HP Data Protector software is automated backup and recovery software for single-server to enterprise environments					
Execute Code	21-April-2016	7.5	HPE Data Protector before 7.03_108, 8.x before 8.15, and 9.x before 9.06 allows remote attackers to execute arbitrary code via unspecified vectors. **Reference** :**CVE-2016-2008**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05085988	A-HP-DATA-30516/37
Execute Code	21-April-2016	10	HPE Data Protector before 7.03_108, 8.x before 8.15, and 9.x before 9.06 allows remote attackers to execute arbitrary code via unspecified vectors, aka ZDI-CAN-3354. **Reference** :**CVE-2016-2007**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05085988	A-HP-DATA-30516/38
Execute Code	21-April-2016	10	HPE Data Protector before 7.03_108, 8.x before 8.15, and 9.x before 9.06 allows remote attackers to execute arbitrary code via unspecified vectors, aka ZDI-CAN-3353. **Reference** :**CVE-2016-**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05085988	A-HP-DATA-30516/39

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			2006		
Execute Code	21-April-2016	10	HPE Data Protector before 7.03_108, 8.x before 8.15, and 9.x before 9.06 allows remote attackers to execute arbitrary code via unspecified vectors, aka ZDI-CAN-3352. **Reference** :**CVE-2016-2005**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05085988	A-HP-DATA-30516/40
Execute Code	21-April-2016	9.3	HPE Data Protector before 7.03_108, 8.x before 8.15, and 9.x before 9.06 allows remote attackers to execute arbitrary code via unspecified vectors. **Reference** :**CVE-2016-2004**		A-HP-DATA-30516/41
Huawei					
Ar3200 Firmware Huawei AR2200 Series Enterprise Routers providing flexible, scalable, and secure switching and routing for converged wired and wireless 3G LTE networks					
Denial of Service	18-April-2016	6.8	Huawei AR3200 routers with software before V200R006C10SPC300 allow remote authenticated users to cause a denial of service (restart) via crafted packets. **Reference** :**CVE-2016-3950**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160406-01-ar-en	A-HUA-AR320-30516/42
Novell					
Service Desk A Service Desk is a primary IT service within the discipline of ITservice management (ITSM) as defined by the Information Technology Infrastructure Library (ITIL).					
Gain Information	22-April-	4	LiveTime/WebObjects/Liv	https://www.	A-NOV-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
	2016		eTime.woa/wa/DownloadAction/downloadFile in Micro Focus Novell Service Desk before 7.2 allows remote authenticated users to conduct Hibernate Que **Reference** : **CVE-2016-1595**	novell.com/support/kb/doc.php?id=7017430	SERVI-30516/43
Gain Information	22-April-2016	4	LiveTime/WebObjects/LiveTime.woa/wa/DownloadAction/downloadFile in Micro Focus Novell Service Desk before 7.2 allows remote authenticated users to conduct Hibernate Query Language (HQL) injection attacks and obtain sensitive information via the entityName parameter. **Reference** :**CVE-2016-1595**	https://www.novell.com/support/kb/doc.php?id=7017430	A-NOV-SERVI-30516/44
Gain Information	22-April-2016	4	Micro Focus Novell Service Desk before 7.2 allows remote authenticated users to read arbitrary attachments via a request to a LiveTime.woa URL, as demonstrated by obtaining sensitive information via a (1) downloadLogFiles or (2) downloadFile action. **Reference** :**CVE-2016-1594**	https://www.novell.com/support/kb/doc.php?id=7017429	A-NOV-SERVI-30516/45
Dir. Trav.	22-April-	6.5	Directory traversal	https://www.	A-NOV-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
	2016		vulnerability in the import users feature in Micro Focus Novell Service Desk before 7.2 allows remote authenticated administrators to upload and execute arbitrary JSP files via a .. (dot dot) in a filename within a multipart/form-data POST request to a LiveTime.woa URL. **Reference** :**CVE-2016-1593**	novell.com/support/kb/doc.php?id=7017428	SERVI-30516/46
Cross Site Scripting	22-April-2016	3.5	Multiple cross-site scripting (XSS) vulnerabilities in Micro Focus Novell Service Desk before 7.2 allow remote authenticated users to inject arbitrary web script or HTML via a certain (1) user name, (2) tf_aClientFirstName, (3) tf_aClientLastName, (4) ta_selectedTopicContent, (5) tf_orgUnitName, (6) tf_aManufacturerFullName, (7) tf_aManufacturerName, (8) tf_aManufacturerAddress, or (9) tf_aManufacturerCity parameter. **Reference** :**CVE-2016-1596**	https://www.novell.com/support/kb/doc.php?id=7017431	A-NOV-SERVI-30516/47
Cross Site Scripting	22-April-	3.5	Multiple cross-site	https://www.	A-NOV-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
	2016		scripting (XSS) vulnerabilities in Micro Focus Novell Service Desk before 7.2 allow remote authenticated users to inject arbitrary web script or HTML via a certain (1) user name, (2) tf_aClientFirstName, (3) tf_aClientLastName, (4) ta_selectedTopicContent, (5) tf_orgUnitName, (6) tf_aManufacturerFullName, (7) tf_aManufacturerName, (8) tf_aManufacturerAddress, or (9) tf_aManufacturerCity parameter. **Reference :CVE-2016-1596**	novell.com/support/kb/doc.php?id=7017431	SERVI-30516/48
Oracle					
Agile Engineering Data Management Agile Engineering Data Management (e6) comprehensively supports all product-related enterprise processes for organizations in industrial manufacturing sectors.					
NA	21-April-2016	1.8	Unspecified vulnerability in the Oracle Agile Engineering Data Management component in Oracle Supply Chain Products Suite 6.1.3.0 and 6.2.0.0 allows remote attackers to affect availability via vectors related to Engineering Communication	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-AGILE-30516/49

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Interface. **Reference :CVE-2016-3428**		
NA	21-April-2016	3.6	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.1.1, 9.3.1.2, 9.3.2, and 9.3.3 allows remote authenticated users to affect confidentiality and integrity via vectors related to Security, a different vulnerability than CVE-2016-3420. **Reference :CVE-2016-3431**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-AGILE-30516/50
NA	21-April-2016	3.6	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.1.1, 9.3.1.2, 9.3.2, and 9.3.3 allows remote authenticated users to affect confidentiality and integrity via vectors related to Security, a different vulnerability than CVE-2016-3431. **Reference :CVE-2016-3420**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-AGILE-30516/51
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 12.1.3, 12.2.3, 12.2.4, and 12.2.5 allows remote	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.htm	A-ORA-APPLI-30516/52

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			attackers to affect integrity via vectors related to Logout. **Reference** :**CVE-2016-3434**	l	
NA	21-April-2016	3.6	Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 12.1.3, 12.2.3, 12.2.4, and 12.2.5 allows local users to affect confidentiality and integrity via unknown vectors. **Reference** :**CVE-2016-0697**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-APPLI-30516/53
NA	21-April-2016	2.6	Unspecified vulnerability in the Oracle Applications Framework component in Oracle E-Business Suite 12.1.3, 12.2.3, 12.2.4, and 12.2.5 allows remote attackers to affect confidentiality and integrity via vectors related to OAF Core. **Reference** :**CVE-2016-3447**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-APPLI-30516/54
NA	21-April-2016	5.8	Unspecified vulnerability in the Oracle Business Intelligence Enterprise Edition component in Oracle Fusion Middleware 11.1.1.7.0, 11.1.1.9.0, and 12.2.1.0.0 allows remote attackers to affect confidentiality and	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-BUSIN-30516/55

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			integrity via vectors related to Analytics Scorecard. **Reference** :**CVE-2016-0479**		
NA	21-April-2016	3.5	Unspecified vulnerability in the Oracle Business Intelligence Enterprise Edition component in Oracle Fusion Middleware 11.1.1.7.0, 11.1.1.9.0, and 12.2.1.0.0 allows remote authenticated users to affect confidentiality and integrity via vectors related to Analytics Web General. **Reference** :**CVE-2016-0468**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-BUSIN-30516/56
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle Common Applications Calendar component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Tasks. **Reference** :**CVE-2016-3436**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-COMMO-30516/57
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul component in Oracle Supply Chain Products Suite 12.1.1, 12.1.2, and 12.1.3 allows remote	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-COMPL-30516/58

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			attackers to affect confidentiality and integrity via vectors related to Dialog Box. **Reference :CVE-2016-3456**		
NA	21-April-2016	6.4	Unspecified vulnerability in the Oracle Configurator component in Oracle Supply Chain Products Suite 12.0.6, 12.1, and 12.2 allows remote attackers to affect confidentiality and integrity via vectors related to JRAD Heartbeat. **Reference :CVE-2016-3438**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-CONFI-30516/59
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle CRM Wireless component in Oracle E-Business Suite 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Call Phone Number Page. **Reference :CVE-2016-3439**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-CRMT-30516/60
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle CRM Wireless component in Oracle E-Business Suite 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Person	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-CRMT-30516/61

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Address Page. **Reference :CVE-2016-3437**		
NA	21-April-2016	7.6	Unspecified vulnerability in the Java VM component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. **Reference :CVE-2016-3454**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-DATAB-30516/62
NA	21-April-2016	4	Unspecified vulnerability in the RDBMS Security component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows local users to affect integrity via unknown vectors, a different vulnerability than CVE-2016-0690. **Reference :CVE-2016-0691**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-DATAB-30516/63
NA	21-April-2016	4	Unspecified vulnerability in the RDBMS Security component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows local users to affect integrity via unknown vectors, a different vulnerability than CVE-2016-0691. **Reference :CVE-2016-0690**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-DATAB-30516/64
NA	21-April-	5	Unspecified vulnerability	http://www.or	A-ORA-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
	2016		in the RDBMS Security component in Oracle Database Server 12.1.0.1 and 12.1.0.2 allows remote attackers to affect availability via unknown vectors. **Reference** :**CVE-2016-0677**	acle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	DATAB-30516/65
NA	21-April-2016	6.4	Unspecified vulnerability in the Oracle Field Service component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Wireless. **Reference** :**CVE-2016-3466**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-FIELD-30516/66
NA	21-April-2016	4	Unspecified vulnerability in the Oracle FLEXCUBE Direct Banking component in Oracle Financial Services Software 12.0.3 allows remote authenticated users to affect confidentiality via vectors related to Accounts. **Reference** :**CVE-2016-3464**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-FLEXC-30516/67
NA	21-April-2016	5	Unspecified vulnerability in the Oracle FLEXCUBE Direct Banking component in Oracle Financial Services Software 12.0.3 allows	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-	A-ORA-FLEXC-30516/68

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			remote attackers to affect confidentiality and integrity via vectors related to Pre-Login. **Reference** :**CVE-2016-3463**	2985753.html	
NA	21-April-2016	9.4	Unspecified vulnerability in the Oracle FLEXCUBE Direct Banking component in Oracle Financial Services Software 12.0.2 and 12.0.3 allows remote attackers to affect confidentiality and integrity via vectors related to the Login sub-component. **Reference** :**CVE-2016-0699**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-FLEXC-30516/69
NA	21-April-2016	5	Unspecified vulnerability in the Oracle FLEXCUBE Direct Banking component in Oracle Financial Services Software 12.0.2 and 12.0.3 allows remote attackers to affect confidentiality and integrity via vectors related to Pre-Login. **Reference** :**CVE-2016-0672**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-FLEXC-30516/70
NA	21-April-2016	2.6	Unspecified vulnerability in the Oracle HTTP Server component in Oracle Fusion Middleware 12.1.2.0 allows remote attackers to affect confidentiality	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.htm	A-ORA-HTTP -30516/71

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
			via vectors related to OSSL Module. **Reference :CVE-2016-0671**	l	
NA	21-April-2016	7.6	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Deployment. **Reference :CVE-2016-3449**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-JDK;J-30516/72
NA	21-April-2016	10	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to 2D. **Reference :CVE-2016-3443**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-JDK;J-30516/73
NA	21-April-2016	4.3	Unspecified vulnerability in Oracle Java SE 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality via vectors related to JCE. **Reference :CVE-2016-3426**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-JDK;J-30516/74
NA	21-April-2016	5	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 allows remote attackers to affect availability via vectors related to 2D. **Reference :CVE-2016-**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.htm	A-ORA-JDK;J-30516/75

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
			3422	l	
NA	21-April-2016	10	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to the Hotspot sub-component. **Reference** :**CVE-2016-0687**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-JDK;J-30516/76
NA	21-April-2016	10	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Serialization. **Reference** :**CVE-2016-0686**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-JDK;J-30516/77
NA	21-April-2016	10	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX. **Reference** :**CVE-2016-3427**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-JDK;J-30516/78
NA	21-April-2016	5	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and	http://www.oracle.com/technetwork/security-	A-ORA-JDK;J-30516/79

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			JRockit R28.3.9 allows remote attackers to affect availability via vectors related to JAXP. **Reference :CVE-2016-3425**	advisory/cpuapr2016v3-2985753.html	
NA	21-April-2016	2.6	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality via vectors related to Security. **Reference :CVE-2016-0695**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-JDK;J-30516/80
NA	21-April-2016	1.7	Unspecified vulnerability in Oracle MySQL 5.6.28 and earlier and 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB. **Reference :CVE-2016-0668**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/81
NA	21-April-2016	2.8	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Locking. **Reference :CVE-2016-0667**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/82
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-	A-ORA-MYSQL-30516/83

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			vectors related to Security: Privileges. **Reference** :**CVE-2016-0666**	2985753.html	
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.6.28 and earlier and 5.7.10 and earlier allows local users to affect availability via vectors related to Security: Encryption. **Reference** :**CVE-2016-0665**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/84
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Performance Schema. **Reference** :**CVE-2016-0663**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/85
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Partition. **Reference** :**CVE-2016-0662**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/86
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.6.28 and earlier and 5.7.10 and earlier allows local users to affect availability via vectors related to Options. **Reference** :**CVE-2016-0661**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/87

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Optimizer. **Reference** :**CVE-2016-0659**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/88
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Optimizer. **Reference** :**CVE-2016-0658**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/89
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect confidentiality via vectors related to JSON. **Reference** :**CVE-2016-0657**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/90
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0654. **Reference** :**CVE-2016-0656**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/91
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier allows local users to affect availability via vectors	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-	A-ORA-MYSQL-30516/92

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			related to InnoDB. **Reference** :**CVE-2016-0655**	2985753.html	
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0656. **Reference** :**CVE-2016-0654**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/93
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to FTS. **Reference** :**CVE-2016-0653**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/94
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to DML. **Reference** :CVE-2016-0652	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/95
NA	21-April-2016	3.5	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier allows local users to affect availability via vectors related to Optimizer. **Reference** : **CVE-2016-0651**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/96
NA	21-April-2016	4	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and	http://www.oracle.com/technetwork/sec	A-ORA-MYSQL-30516/97

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
			earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to Replication. **Reference :CVE-2016-0650**	urity-advisory/cpuapr2016v3-2985753.html	
NA	21-April-2016	4	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to PS. **Reference :CVE-2016-0649**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/98
NA	21-April-2016	4	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to PS. **Reference :CVE-2016-0648**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/99
NA	21-April-2016	4	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to FTS. **Reference :CVE-2016-0647**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/100
NA	21-April-2016	4	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-	A-ORA-MYSQL-30516/101

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			vectors related to DML. **Reference :CVE-2016-0646**	2985753.html	
NA	21-April-2016	4	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to DDL. **Reference :CVE-2016-0644**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/102
NA	21-April-2016	4	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect confidentiality via vectors related to DML. **Reference :CVE-2016-0643**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/103
NA	21-April-2016	4.3	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect integrity and availability via vectors related to Federated. **Reference :CVE-2016-0642**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/104
NA	21-April-2016	4.9	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect confidentiality and availability via vectors related to	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/105

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			MyISAM. **Reference** :**CVE-2016-0641**		
NA	21-April-2016	4.9	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect integrity and availability via vectors related to DML. **Reference** :**CVE-2016-0640**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/106
NA	21-April-2016	10	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Pluggable Authentication. **Reference** :**CVE-2016-0639**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/107
NA	21-April-2016	4.3	Unspecified vulnerability in the MySQL Enterprise Monitor component in Oracle MySQL 3.0.25 and earlier and 3.1.2 and earlier allows remote administrators to affect confidentiality, integrity, and availability via vectors related to Monitoring: Server. **Reference** :**CVE-2016-3461**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-MYSQL-30516/108
NA	21-April-2016	6.5	Unspecified vulnerability in the Oracle OLAP	http://www.oracle.com/tec	A-ORA-OLAP-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows local users to affect confidentiality, integrity, and availability via unspecified vectors. **Reference** :**CVE-2016-0681**	hnetwork/security-advisory/cpuapr2016v3-2985753.html	30516/109
NA	21-April-2016	6.9	Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0682, CVE-2016-0689, CVE-2016-0692, and CVE-2016-0694. **Reference** :**CVE-2016-3418**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-ORACL-30516/110
NA	21-April-2016	6.9	Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-ORACL-30516/111

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			than CVE-2016-0682, CVE-2016-0689, CVE-2016-0692, and CVE-2016-3418. **Reference** :**CVE-2016-0694**		
NA	21-April-2016	6.9	Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0682, CVE-2016-0689, CVE-2016-0694, and CVE-2016-3418. **Reference** :**CVE-2016-0692**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-ORACL-30516/112
NA	21-April-2016	6.9	Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0682, CVE-2016-0692, CVE-2016-0694, and CVE-2016-3418.	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-ORACL-30516/113

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
NA	21-April-2016	6.9	**Reference** :**CVE-2016-0689** Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0689, CVE-2016-0692, CVE-2016-0694, and CVE-2016-3418. **Reference** :**CVE-2016-0682**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-ORACL-30516/114
NA	21-April-2016	9	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.5.0, 8.5.1, and 8.5.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters. **Reference** :**CVE-2016-3455**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-OUTSI-30516/115

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
NA	21-April-2016	5.5	Unspecified vulnerability in the PeopleSoft Enterprise HCM component in Oracle PeopleSoft Products 9.2 allows remote authenticated users to affect confidentiality and integrity via vectors related to ePerformance. **Reference** :**CVE-2016-3460**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/116
NA	21-April-2016	4.9	Unspecified vulnerability in the PeopleSoft Enterprise HCM ePerformance component in Oracle PeopleSoft Products 9.2 allows remote authenticated users to affect confidentiality and integrity via vectors related to Security. **Reference** :**CVE-2016-3457**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/117
NA	21-April-2016	4	Unspecified vulnerability in the PeopleSoft Enterprise HCM component in Oracle PeopleSoft Products 9.1 and 9.2 allows remote authenticated users to affect confidentiality via vectors related to Fusion HR Talent Integration. **Reference** :**CVE-2016-0407**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/118
NA	21-April-2016	4.3	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools	http://www.oracle.com/technetwork/sec	A-ORA-PEOPL-30516/119

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to Portal. **Reference :CVE-2016-3442**	urity-advisory/cpuapr2016v3-2985753.html	
NA	21-April-2016	4.3	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote attackers to affect availability via vectors related to PIA Core Technology. **Reference :CVE-2016-3435**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/120
NA	21-April-2016	3.5	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to Rich Text Editor, a different vulnerability than CVE-2016-0698. **Reference :CVE-2016-3423**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/121
NA	21-April-2016	6.5	Unspecified vulnerability in the PeopleSoft	http://www.oracle.com/tec	A-ORA-PEOPL-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to Activity Guide. **Reference** :**CVE-2016-3421**	hnetwork/security-advisory/cpuapr2016v3-2985753.html	30516/122
NA	21-April-2016	4.3	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to PIA Search Functionality. **Reference** :**CVE-2016-3417**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/123
NA	21-April-2016	4.3	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to Rich Text Editor, a different vulnerability than CVE-2016-3423.	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/124

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-2016-0698**		
NA	21-April-2016	5.5	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to File Processing. **Reference** :**CVE-2016-0685**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/125
NA	21-April-2016	4	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to Search Framework. **Reference** : **CVE-2016-0683**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/126
NA	21-April-2016	5.5	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote authenticated users to affect integrity and availability via vectors	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/127

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
			related to PIA Grids. **Reference** :**CVE-2016-0679**		
NA	21-April-2016	4.3	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53 through 8.55 allows remote authenticated users to affect confidentiality and integrity via vectors related to the Activity Guide sub-component. **Reference** :**CVE-2016-0408**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/128
NA	21-April-2016	5.5	Unspecified vulnerability in the PeopleSoft Enterprise SCM component in Oracle PeopleSoft Products 9.1 and 9.2 allows remote authenticated users to affect confidentiality and integrity via vectors related to Services Procurement. **Reference** :**CVE-2016-0680**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-PEOPL-30516/129
NA	21-April-2016	5.4	Unspecified vulnerability in the Oracle Retail Xstore Point of Service component in Oracle Retail Applications 5.0, 5.5, 6.0, 6.5, 7.0, and 7.1 allows remote authenticated users to affect confidentiality and integrity via vectors	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-RETAI-30516/130

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			related to Xstore Services. **Reference** :**CVE-2016-3429**		
NA	21-April-2016	3.2	Unspecified vulnerability in the Siebel Core - Common Components component in Oracle Siebel CRM 8.1.1 and 8.2.2 allows local users to affect confidentiality and integrity via vectors related to Email. **Reference** :**CVE-2016-0674**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-SIEBE-30516/131
NA	21-April-2016	4.9	Unspecified vulnerability in the Siebel UI Framework component in Oracle Siebel CRM 8.1.1 and 8.2.2 allows remote authenticated users to affect confidentiality and integrity via vectors related to UIF Open UI. **Reference** :**CVE-2016-0673**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-SIEBE-30516/132
NA	21-April-2016	4.3	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows remote attackers to affect integrity via vectors related to the Automated Installer sub-component. **Reference** :**CVE-2016-0623**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-SOLAR-30516/133
NA	21-April-2016	4.9	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users	http://www.oracle.com/technetwork/sec	A-ORA-SOLAR-30516/134

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			to affect availability via vectors related to ZFS. **Reference** :**CVE-2016-3465**	urity-advisory/cpuapr2016v3-2985753.html	
NA	21-April-2016	7.2	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows local users to affect confidentiality, integrity, and availability via vectors related to Filesystem. **Reference** :**CVE-2016-3441**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-SOLAR-30516/135
NA	21-April-2016	2.1	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows local users to affect availability via vectors related to Filesystem. **Reference** :**CVE-2016-3419**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-SOLAR-30516/136
NA	21-April-2016	4.1	Unspecified vulnerability in the Oracle VM VirtualBox component in Oracle Virtualization VirtualBox before 5.0.18 allows local users to affect confidentiality, integrity, and availability via vectors related to Core. **Reference** :**CVE-2016-0678**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-VM VI-30516/137
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6,	http://www.oracle.com/technetwork/security-advisory/cpu	A-ORA-WEBLO-30516/138

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			12.1.2, 12.1.3, and 12.2.1 allows remote attackers to affect confidentiality and integrity via vectors related to Console. **Reference :CVE-2016-3416**	apr2016v3-2985753.html	
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Console, a different vulnerability than CVE-2016-0675. **Reference :CVE-2016-0700**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-WEBLO-30516/139
NA	21-April-2016	6.4	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6 allows remote attackers to affect confidentiality and integrity via vectors related to Console. **Reference :CVE-2016-0696**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-WEBLO-30516/140
NA	21-April-2016	2.6	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6, 12.1.2, and 12.1.3 allows remote attackers	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.htm	A-ORA-WEBLO-30516/141

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			to affect integrity via vectors related to Core Components. **Reference** :**CVE-2016-0688**	l	
NA	21-April-2016	4.3	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Console, a different vulnerability than CVE-2016-0700. **Reference** :**CVE-2016-0675**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-WEBLO-30516/142
NA	21-April-2016	7.5	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6, 12.1.2, 12.1.3, and 12.2.1 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Java Messaging Service. **Reference** :**CVE-2016-0638**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-ORA-WEBLO-30516/143
Panda					
Gain Privileges	18-April-2016	7.2	Panda Endpoint Administration Agent before 7.50.00, as used in Panda Security for Business products for		A-PAN-PANDA-30516/144

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Windows, uses a weak ACL for the Panda Security/WaAgent directory and sub-directories, which allows local users to gain SYSTEM privileges by modifying an executable module. **Reference** :**CVE-2016-3943**		
Gain Privileges	18-April-2016	7.2	Panda Security URL Filtering before 4.3.1.9 uses a weak ACL for the "Panda Security URL Filtering" directory and installed files, which allows local users to gain SYSTEM privileges by modifying Panda_URL_Filteringb.exe. **Reference** :**CVE-2015-7378**		A-PAN-PANDA-30516/145
Qemu					
Qemu QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization					
Denail of Service;Execute Code; Overflow; Memory Corruption	26-April-2016	6.8	Buffer overflow in the mipsnet_receive function in hw/net/mipsnet.c in QEMU, when the guest NIC is configured to accept large packets, allows remote attackers to cause a denial of service (memory corruption and QEMU crash) or possibly	https://bugzilla.redhat.com/show_bug.cgi?id=1326082	A-QEM-QEMU-30516/146

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
			execute arbitrary code via a packet larger than 1514 bytes. **Reference** :**CVE-2016-4002**		
Samba					
Samba Samba is a re-implementation of the SMB/CIFS networking protocol, it facilitates file and printer sharing among Linux and Windows systems as an alternative to NFS.					
Gain Information	24-April-2016	5.8	Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not verify X.509 certificates from TLS servers, which allows man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a crafted certificate. **Reference** :**CVE-2016-2113**	https://www.samba.org/samba/security/CVE-2016-2113.html	A-SAM-SAMBA-30516/147
Gain Information	24-April-2016	4.3	The NETLOGON service 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, when a domain controller is configured, allows remote attackers to spoof the computer name of a secure channel's endpoint, and obtain sensitive session information, by running a crafted application and leveraging the ability to sniff network traffic, a	https://www.samba.org/samba/security/CVE-2016-2111.html	A-SAM-SAMBA-30516/148

Product/ Vulnerability Type(s)	**Publish Date**	**CVSS**	**Vulnerability Description**	**Patch(if any)**	**NCIIPC ID**
			related issue to CVE-2015-0005. **Reference** :**CVE-2016-2111**		
Denail of Service;Execute Code	24-April-2016	4.3	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 does not properly implement the DCE-RPC layer, which allows remote attackers to perform protocol-downgrade attacks, cause a denial of service (application crash or CPU consumption), or possibly execute arbitrary code on a client system via unspecified vectors. **Reference** :**CVE-2015-5370**	https://www.samba.org/samba/security/CVE-2015-5370.html	A-SAM-SAMBA-30516/149
NA	24-April-2016	4.3	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 does not require SMB signing within a DCERPC session over ncacn_np, which allows man-in-the-middle attackers to spoof SMB clients by modifying the client-server data stream. **Reference** :**CVE-2016-2115**	https://www.samba.org/samba/security/CVE-2016-2115.html	A-SAM-SAMBA-30516/150
NA	24-April-2016	4.3	The SMB1 protocol implementation in Samba 4.x before 4.2.11, 4.3.x before	https://www.samba.org/samba/security/CVE-2016-	A-SAM-SAMBA-30516/151

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			4.3.8, and 4.4.x before 4.4.2 does not recognize the "server signing = mandatory" setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying the client-server data stream. **Reference** : **CVE-2016-2114**	2114.html	
NA	24-April-2016	4.3	The bundled LDAP client library 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 does not recognize the "client ldap sasl wrapping" setting, which allows man-in-the-middle attackers to perform LDAP protocol-downgrade attacks by modifying the client-server data stream. **Reference** : **CVE-2016-2112**	https://www.samba.org/samba/security/CVE-2016-2112.html	A-SAM-SAMBA-30516/152
NA	24-April-2016	4.3	The NTLMSSP authentication implementation 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 allows man-in-the-middle attackers to perform protocol-downgrade attacks by modifying the client-server data stream to remove application-layer	https://www.samba.org/samba/security/CVE-2016-2110.html	A-SAM-SAMBA-30516/153

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			flags or encryption settings, as demonstrated by clearing the NTLMSSP_NEGOTIATE_SEAL or NTLMSSP_NEGOTIATE_SIGN option to disrupt LDAP security. **Reference** :**CVE-2016-2110**		
Sierra Wireless					
Aleos ALEOS Application Framework (AAF) provides developers a complete set of building blocks and tools for creating applications that run inside Sierra Wireless AirLink Gateways.					
NA	21-April-2016	4.3	ACEmanager in Sierra Wireless ALEOS 4.4.2 and earlier on ES440, ES450, GX400, GX440, GX450, and LS300 devices allows remote attackers to read the filteredlogs.txt file, and consequently discover potentially sensitive boot-sequence information, via unspecified vectors. **Reference** :**CVE-2015-6479**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-01	A-SIE-ALEOS-30516/154
Squid-cache					
Squid Squid is a caching and forwarding web proxy					
Denial of Service	19-April-2016	4.3	The FwdState::connectedToPeer method in FwdState.cc in Squid before 3.5.14 and 4.0.x before 4.0.6 does not	http://www.squid-cache.org/Advisories/SQUID-2016_1.txt	A-SQU-SQUID-30516/155

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			properly handle SSL handshake errors when built with the --with-openssl option, which allows remote attackers to cause a denial of service (application crash) via a plaintext HTTP message. **Reference** :**CVE-2016-2390**		
Denail of Service;Execute Code;Overflow	25-April-2016	6.8	Multiple stack-based buffer overflows in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote HTTP servers to cause a denial of service or execute arbitrary code via crafted Edge Side Includes (ESI) responses. **Reference** :**CVE-2016-4052**	http://www.squid-cache.org/Advisories/SQUID-2016_6.txt	A-SQU-SQUID-30516/156
Denail of Service;Execute Code;Overflow	25-April-2016	6.8	Buffer overflow in cachemgr.cgi in Squid 2.x, 3.x before 3.5.17, and 4.x before 4.0.9 might allow remote attackers to cause a denial of service or execute arbitrary code by seeding manager reports with crafted data. **Reference** :**CVE-2016-4051**	http://www.squid-cache.org/Advisories/SQUID-2016_5.txt	A-SQU-SQUID-30516/157
Execute Code; Overflow	25-April-2016	6.8	Buffer overflow in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allows remote attackers to	http://www.squid-cache.org/Advisories/SQUI	A-SQU-SQUID-30516/158

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
			execute arbitrary code via crafted Edge Side Includes (ESI) responses. **Reference** :**CVE-2016-4054**	D-2016_6.txt	
Overflow; Gain Information	25-April-2016	4.3	Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote attackers to obtain sensitive stack layout information via crafted Edge Side Includes (ESI) responses, related to incorrect use of assert and compiler optimization. **Reference** :**CVE-2016-4053**	http://www.squid-cache.org/Advisories/SQUID-2016_6.txt	A-SQU-SQUID-30516/159
Symantec					
Altiris It Management Suite Altiris Client Management Suite 8 from Symantec manages, secures and troubleshoots systems with greater efficiency on more platforms, including Windows, Mac, Linux and virtual desktop environments.					
Bypass	20-April-2016	2.1	The Inventory Solution component in the Management Agent in the client in Symantec Altiris IT Management Suite (ITMS) through 7.6 HF7 allows local users to bypass intended application-blacklist restrictions via unspecified vectors. **Reference** :**CVE-2016-2202**	https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160407_00	A-SYM-ALTIR-30516/160
Gain Information	22-April-2016	2.1	The management console on Symantec Messaging Gateway (SMG) Appliance devices	http://www.symantec.com/security_response/sec	A-SYM-MESSA-30516/161

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			before 10.6.1 allows local users to discover an encrypted AD password by leveraging certain read privileges. **Reference :CVE-2016-2203**	urityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160418_00	
NA	22-April-2016	6.5	The management console on Symantec Messaging Gateway (SMG) Appliance devices before 10.6.1 allows local users to obtain root-shell access via crafted terminal-window input. **Reference :CVE-2016-2204**	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160418_00	A-SYM-MESSA-30516/162
Tibco					
Enterprise Message Service; Enterprise Message Service Appliance a drop-in, standalone solution for enterprise messaging.					
Denail of Service;Execute Code;Overflow	20-April-2016	6.5	Buffer overflow in tibemsd in the server in TIBCO Enterprise Message Service (EMS) before 8.3.0 and EMS Appliance before 2.4.0 allows remote authenticated users to cause a denial of service or possibly execute arbitrary code via crafted inbound data. **Reference : CVE-2016-3628**	http://www.tibco.com/assets/blt8a2d9978616c21fe/2016-001-advisory.txt	A-TIB-ENTER-30516/163
Wireshark					
Wireshark					

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
Wireshark is a network protocol analyzer for Unix and Windows.					
Denial of Service	25-April-2016	4.3	epan/dissectors/packet-mswsp.c in the MS-WSP dissector in Wireshark 2.0.x before 2.0.3 does not ensure that data is available before array allocation, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference** :**CVE-2016-4083**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=66417b17b3570b163a16ca81f71ce5bcb10548d2	A-WIR-WIRES-30516/164
Denial of Service	25-April-2016	4.3	epan/dissectors/packet-iax2.c in the IAX2 dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet. **Reference** : **CVE-2016-4081**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=42f299be6abb302f32cec78b1c0812364c9f9285	A-WIR-WIRES-30516/165
Denial of Service	25-April-2016	4.3	The IEEE 802.11 dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 does not properly restrict element lists, which allows remote attackers to cause a denial of service (deep recursion and application crash) via a crafted packet, related to	http://www.wireshark.org/security/wnpa-sec-2016-21.html	A-WIR-WIRES-30516/166

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			epan/dissectors/packet-capwap.c and epan/dissectors/packet-ieee80211.c. **Reference** :**CVE-2016-4078**		
Denial of Service	25-April-2016	4.3	epan/reassemble.c in TShark in Wireshark 2.0.x before 2.0.3 relies on incorrect special-case handling of truncated Tvb data structures, which allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted packet. **Reference** :**CVE-2016-4077**	http://www.wireshark.org/security/wnpa-sec-2016-20.html	A-WIR-WIRES-30516/167
Denial of Service	25-April-2016	4.3	epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 2.0.x before 2.0.3 does not properly initialize memory for search patterns, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference** :**CVE-2016-4076**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=ea8e6955fcff21333c203bc00f69d5025761459b	A-WIR-WIRES-30516/168
Denail of Service Overflow	25-April-2016	4.3	Stack-based buffer overflow in epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 1.12.x before 1.12.11 allows remote attackers	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=99efcb0f	A-WIR-WIRES-30516/169

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			to cause a denial of service (application crash) or possibly have unspecified other impact via a long string in a packet. **Reference** :**CVE-2016-4085**	5aeeb4b2179e88c7a4233022aaeecf0b	
Denail of Service Overflow	25-April-2016	4.3	Integer signedness error in epan/dissectors/packet-mswsp.c in the MS-WSP dissector in Wireshark 2.0.x before 2.0.3 allows remote attackers to cause a denial of service (integer overflow and application crash) via a crafted packet that triggers an unexpected array size. **Reference** :**CVE-2016-4084**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=66417b17b3570b163a16ca81f71ce5bcb10548d2	A-WIR-WIRES-30516/170
Denail of Service Overflow	25-April-2016	4.3	epan/dissectors/packet-gsm_cbch.c in the GSM CBCH dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 uses the wrong variable to index an array, which allows remote attackers to cause a denial of service (out-of-bounds access and application crash) via a crafted packet. **Reference** : **CVE-2016-4082**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=0fe522dfc689c3ebd119f2a6775d1f275c5f04d8	A-WIR-WIRES-30516/172
Denail of Service Overflow	25-April-2016	4.3	epan/dissectors/packet-pktc.c in the PKTC	https://code.wireshark.or	A-WIR-WIRES-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 misparses timestamp fields, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet. **Reference** :**CVE-2016-4080**	g/review/gitweb?p=wireshark.git;a=commit;h=ad097385c05c370440fb810e67f811398efc0ea0	30516/173
Denail of Service Overflow	25-April-2016	4.3	epan/dissectors/packet-pktc.c in the PKTC dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 does not verify BER identifiers, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) via a crafted packet. **Reference** :**CVE-2016-4079**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=4cdc9eeba58f866bd5f273e9c5b3876857a7a4bf	A-WIR-WIRES-30516/174
Denail of Service Overflow	25-April-2016	4.3	epan/proto.c in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 does not limit the protocol-tree depth, which allows remote attackers to cause a denial of service (stack memory consumption and application crash) via a crafted packet. **Reference** : **CVE-2016-4006**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=8dc9551e1d56290e6f7f02cc38b77e1d211fd4a5	A-WIR-WIRES-30516/175

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Application/Operating System					
Bouncycastle/Google					
Legion-of-the-bouncy-castle-java-crytography-api/Android Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel					
Gain Information	17-April-2016	4.3	asn1/cms/GCMParameters.java in the Bouncy Castle Crypto APIs 1.54 for Java, as used in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01, has an improper AES-GCM-ICVlen value, which makes it easier for attackers to defeat a cryptographic protection mechanism and discover an authentication key via a crafted application, aka internal bug 26234568. **Reference** :**CVE-2016-2427**	http://source.android.com/security/bulletin/2016-04-02.html	A-O-BOU-LEGIO-30516/176
Cisco/Cisco					
Adaptive Security Appliance Software;Jabber Software Development Kit;Libsrtp;Unified Communications Manager;Unity Connection;Webex Meeting Center/Dx Series Ip Phones Firmware;Ios Xe;Ip Phone 7800 Series Firmware;Ip Phone 8800 Series Firmware;Unified Ip Phone 6900 Series Firmware;Unified Ip Phone 7900 Series Firmware;Unified Ip Phone 8900 Series Firmware;Unified Wireless Ip Phone 7920 Firmware Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.					
Denail of Service Overflow	21-April-2016	7.8	The encryption-processing feature in Cisco libSRTP before 1.5.3 allows remote attackers to cause a denial of service via crafted fields in SRTP	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-	A-CIS-ADAPT-30516/177

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			packets, aka Bug ID CSCux00686. **Reference** :**CVE-2015-6360**	libsrtp	
Dhcpcd Project/Google					
Dhcpcd/Android Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel					
Denail of Service;Execute Code;Overflow	17-April-2016	10	dhcpcd before 6.10.0, as used in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 and other products, mismanages option lengths, which allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow) via a malformed DHCP response, aka internal bug 26461634. **Reference** :**CVE-2016-1503**	https://android.googlesource.com/platform/external/dhcpcd/+/1390ace71179f04a09c300ee8d0300aa69d9db09	A-DHC-DHCPC-30516/178
Fedoraproject/Redhat					
389 Directory Server/Enterprise Linux;Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation Red Hat Enterprise Linux (RHEL) is a Linuxdistribution developed by Red Hat and targeted toward the commercial market.					
Denial of Service	19-April-2016	7.8	slapd/connection.c in 389 Directory Server (formerly Fedora Directory Server) 1.3.4.x before 1.3.4.7 allows remote attackers to cause a denial of service (infinite loop and	https://fedorahosted.org/389/ticket/48412	A-FED-389D-30516/179

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			connection blocking) by leveraging an abnormally closed connection. **Reference** : **CVE-2016-0741**		
Giflib Project/Novell					
Giflib/Opensuse Opensuse is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies					
Denail of Service Overflow	21-April-2016	4.3	Heap-based buffer overflow in util/gif2rgb.c in gif2rgb in giflib 5.1.2 allows remote attackers to cause a denial of service (application crash) via the background color index in a GIF file. **Reference** : **CVE-2016-3977**	https://sourceforge.net/p/giflib/code/ci/ea8dbc5786862a3e16a5acfa3d24e2c2f608cd88/	A-GIF-GIFLI-30516/180
GNU;Suse/Novell;Suse					
Glibc/Linux Enterprise Debuginfo/Opensuse/Linux Enterprise Desktop;Linux Enterprise Server;Linux Enterprise Software Development Kit Opensuse is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies					
Denail of Service;Execute Code;Overflow	19-April-2016	7.5	Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.	https://sourceware.org/bugzilla/show_bug.cgi?id=16962	A-GNU-GLIBC-30516/181

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference :CVE-2014-9761		
Libav/Ubuntu					
Libav/Ubuntu Libav is a complete, cross-platform solution to record, convert and stream audio and video.					
Denial of Service	19-April-2016	4.3	The ff_h263_decode_mba function in libavcodec/ituh263dec.c in Libav before 11.5 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a file with crafted dimensions. **Reference : CVE-2015-5479**	https://git.libav.org/?p=libav.git;a=commitdiff;h=0a49a62f998747cfa564d98d36a459fe70d3299b	A-LIB-LIBAV-30516/182
Libtiff Project/Novell					
Libtiff/Opensuse Opensuse is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies					
Denail of Service Overflow	19-April-2016	5	Buffer overflow in the readextension function in gif2tiff.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (application crash) via a crafted GIF file. **Reference :CVE-2016-3186**	https://bugzilla.redhat.com/show_bug.cgi?id=1319503	A-LIB-LIBTI-30516/183
Canonical/Optipng					
Ubuntu Linux/Optipng A PNG optimizer that recompresses the image files to a smaller size, without losing any information.					
Denail of Service Overflow	20-April-2016	4.3	gifread.c in gif2png, as used in OptiPNG before 0.7.6, allows remote attackers to cause a	http://optipng.sourceforge.net/history.txt	O-CAN-UBUNT-30516/184

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			denial of service (uninitialized memory read) via a crafted GIF file. **Reference** : **CVE-2015-7802**		
Execute Code	20-April-2016	9.3	Use-after-free vulnerability in OptiPNG 0.6.4 allows remote attackers to execute arbitrary code via a crafted PNG file. **Reference** : **CVE-2015-7801**	https://bugzilla.redhat.com/show_bug.cgi?id=1264015	O-CAN-UBUNT-30516/185
Canonical/Videolan					
Ubuntu Linux/Vlc Media Player VLC media player (commonly known as VLC) is a portable, free and open-source, cross-platform media player andstreaming media server written by the VideoLAN project.					
Denail of Service Overflow	18-April-2016	4.3	Buffer overflow in the AStreamPeekStream function in input/stream.c in VideoLAN VLC media player before 2.2.0 allows remote attackers to cause a denial of service (crash) via a crafted wav file, related to "seek across EOF." **Reference** : **CVE-2016-3941**	https://bugs.launchpad.net/ubuntu/+source/vlc/+bug/1533633	O-CAN-UBUNT-30516/186
Canonical;Debian/Gnupg					
Ubuntu Linux/Debian Linux/Libgcrypt Libgcrypt is a general purpose cryptographic library based on the code from GnuPG.					
Gain Information	19-April-2016	1.9	Libgcrypt before 1.6.5 does not properly perform elliptic-point curve multiplication during decryption, which		O-CAN-UBUNT-30516/187

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
		🟩	makes it easier for physically proximate attackers to extract ECDH keys by measuring electromagnetic emanations. **Reference** : **CVE-2015-7511**		
Canonical;Debian;Novell/Xdelta					
Ubuntu Linux/Debian Linux/Opensuse/Xdelta3 Opensuse is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies					
Execute Code; Overflow	19-April-2016	6.8	Buffer overflow in the main_get_appheader function in xdelta3-main.h in xdelta3 before 3.0.9 allows remote attackers to execute arbitrary code via a crafted input file. **Reference** : **CVE-2014-9765**	https://github.com/jmacd/xdelta-devel/commit/ef93ff74203e030073b898c05e8b4860b5d09ef2	O-CAN-UBUNT-30516/188
Debian;Novell;Suse/GNU;Suse					
Debian Linux/Opensuse/Linux Enterprise Desktop;Linux Enterprise Server; Linux Enterprise Software Development Kit/Glibc/Linux Enterprise Debuginfo Opensuse is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies					
Denial of Service;Gain Information	19-April-2016	6.4	The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value. **Reference** : **CVE-2015-8776**	https://sourceware.org/bugzilla/show_bug.cgi?id=18985	O-DEB-DEBIA-30516/189

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denail of Service;Execute Code;Overflow	19-April-2016	7.5	Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name. **Reference** : **CVE-2015-8779**	https://sourceware.org/bugzilla/show_bug.cgi?id=17905	O-DEB-DEBIA-30516/190
Denail of Service;Execute Code;Overflow	19-April-2016	7.5	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access. **Reference** : **CVE-2015-8778**	https://sourceware.org/bugzilla/show_bug.cgi?id=18240	O-DEB-DEBIA-30516/191
Fedoraproject/Latex2rtf					
Fedora/Latex2rtf LaTeX2rtf is a translator program which is intended to translate a LaTeX document (precisely: the text and a limited subset of LaTeX tags) into the RTF format which can be imported by several text processors					
Execute Code	18-April-2016	9.3	Format string vulnerability in the CmdKeywords function in funct1.c in latex2rtf	https://sourceforge.net/p/latex2rtf/code/1244/	O-FED-FEDOR-30516/192

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			before 2.3.10 allows remote attackers to execute arbitrary code via format string specifiers in the \keywords command in a crafted TeX file. **Reference** : **CVE-2015-8106**		
Fedoraproject/Libreswan					
Fedora/Libreswan Libreswan is a *free software* implementation of the most widely supported and standarized VPN protocol based on ("IPsec") and the*Internet Key Exchange* ("IKE").					
Denial of Service	18-April-2016	5	Libreswan 3.16 might allow remote attackers to cause a denial of service (daemon restart) via an IKEv2 aes_xcbc transform. **Reference** : **CVE-2016-3071**	https://libreswan.org/security/CVE-2016-3071/CVE-2016-3071.txt	A-O-FED-FEDOR-30516/193
Operating System					
Accuenergy					
Gain Information	21-April-2016	5	The AXM-NET module in Accuenergy Acuvim II NET Firmware 3.08 and Acuvim IIR NET Firmware 3.08 allows remote attackers to discover a cleartext mail-server password via unspecified vectors. **Reference** : **CVE-2016-2294**	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-02	O-ACC-ACUVI-30516/194
NA	21-April-2016	7.5	The AXM-NET module in Accuenergy Acuvim II NET Firmware 3.08 and Acuvim IIR NET Firmware 3.08 allows remote	https://ics-cert.us-cert.gov/advisories/ICSA-16-105-02	O-ACC-ACUVI-30516/195

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			attackers to discover settings via a direct request to an unspecified URL. **Reference** : **CVE-2016-2293**		
Cisco					
IOS; Ios Xe					
IOS XE represents the continuing evolution of Cisco's pre-eminent IOS operating system					
NA	20-April-2016	5	The NTP implementation in Cisco IOS 15.1 and 15.5 and IOS XE 3.2 through 3.17 allows remote attackers to modify the system time via crafted packets, aka Bug ID CSCux46898. **Reference** : **CVE-2016-1384**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160419-ios	O-CIS-IOS;I-30516/196
Google					
Android					
Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel					
Gain Information	17-April-2016	4.3	server/content/ContentService.java in the Framework component in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not check for a GET_ACCOUNTS permission, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 26094635. **Reference** : **CVE-2016-2426**	https://android.googlesource.com/platform/frameworks/base/+/63363af721650e426db5b0bdfb8b2d4fe36abdb0	O-GOO-ANDRO-30516/197

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
Gain Information	17-April-2016	4.3	mail/compose/ComposeActivity.java in AOSP Mail in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 supports file:///data attachments, which allows attackers to obtain sensitive information via a crafted application, aka internal bugs 7154234 and 26989185. **Reference** : **CVE-2016-2425**	https://android.googlesource.com/platform/packages/apps/UnifiedEmail/+/0d9dfd649bae9c181e3afc5d571903f1eb5dc46f	O-GOO-ANDRO-30516/198
Gain Information	17-April-2016	7.1	exchange/eas/EasAutoDiscover.java in the Autodiscover implementation in Exchange ActiveSync in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 allows attackers to obtain sensitive information via a crafted application that triggers a spoofed response to a GET request, aka internal bug 26488455. **Reference** : **CVE-2016-2415**	https://android.googlesource.com/platform/packages/apps/Exchange/+/0d1a38b1755efe7ed4e8d7302a24186616bba9b2	O-GOO-ANDRO-30516/199
Gain Privileges	17-April-2016	9.3	Wi-Fi in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not prevent use of a Wi-Fi CA certificate in an	https://android.googlesource.com/platform/packages/apps/CertInstaller/+/70dde987	O-GOO-ANDRO-30516/200

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
			unrelated CA role, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26324357. **Reference** : **CVE-2016-2422**	0e9450e10418a32206ac1bb30f036b2c	
Gain Privileges	17-April-2016	9.3	rootdir/init.rc in Android 4.x before 4.4.4 does not ensure that the /data/tombstones directory exists for the Debuggerd component, which allows attackers to gain privileges via a crafted application, aka internal bug 26403620. **Reference** : **CVE-2016-2420**	https://android.googlesource.com/platform/system/core/+/81df1cc77722000f8d0025c1ab00ced123aa573c	O-GOO-ANDRO-30516/201
Gain Privileges	17-April-2016	9.3	media/libmedia/IOMX.cpp in mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not initialize a handle pointer, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26403627. **Reference** : **CVE-2016-2413**	https://android.googlesource.com/platform/frameworks/av/+/25be9ac20db51044e1b09ca67906355e4f328d48	O-GOO-ANDRO-30516/202

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Gain Privileges	17-April-2016	9.3	include/core/SkPostConfig.h in Skia, as used in System_server in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01, mishandles certain crashes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26593930. **Reference** : **CVE-2016-2412**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/203
Gain Privileges	17-April-2016	9.3	A Qualcomm Power Management kernel driver in Android 6.x before 2016-04-01 allows attackers to gain privileges via a crafted application that leverages root access, aka internal bug 26866053. **Reference** : **CVE-2016-2411**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/204
Gain Privileges	17-April-2016	6.9	A Qualcomm video kernel driver in Android 6.x before 2016-04-01 allows attackers to gain privileges via a crafted application that leverages control over a service that can call this driver, aka internal bug	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/205

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**
			26291677. **Reference** : **CVE-2016-2410**		
Gain Privileges	17-April-2016	9.3	A Texas Instruments (TI) haptic kernel driver in Android 6.x before 2016-04-01 allows attackers to gain privileges via a crafted application that leverages control over a service that can call this driver, aka internal bug 25981545. **Reference** : **CVE-2016-2409**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/206
Gain Privileges	17-April-2016	7.2	libs/binder/IMemory.cpp in the IMemory Native Interface in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not properly consider the heap size, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26877992. **Reference** : **CVE-2016-0846**	https://android.googlesource.com/platform/frameworks/native/+/f3199c228aced7858b75a8070b8358c155ae0149	O-GOO-ANDRO-30516/207
Gain Privileges	17-April-2016	7.2	The Qualcomm RF driver in Android 6.x before 2016-04-01 does not properly restrict access to socket ioctl calls, which allows attackers	https://android.googlesource.com/platform/external/sepolicy/+/57531cacb	O-GOO-ANDRO-30516/208

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
			to gain privileges via a crafted application, aka internal bug 26324307. **Reference** : **CVE-2016-0844**	40682be4b1189c721fd1e7f25bf3786	
Gain Privileges	17-April-2016	7.2	The Qualcomm ARM processor performance-event manager in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 allows attackers to gain privileges via a crafted application, aka internal bug 25801197. **Reference** : **CVE-2016-0843**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/209
Bypass	17-April-2016	6.6	server/telecom/CallsManager.java in Telephony in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not properly consider whether a device is provisioned, which allows physically proximate attackers to bypass the Factory Reset Protection protection mechanism and delete data via unspecified vectors, aka internal bug 26303187. **Reference** : **CVE-2016-2423**	https://android.googlesource.com/platform/packages/services/Telecomm/+/a06c9a4aef69ae27b951523cf72bf72412bf48fa	O-GOO-ANDRO-30516/210
Bypass	17-April-2016	6.6	Setup Wizard in Android 5.1.x before 5.1.1 and 6.x before 2016-04-01	http://source.android.com/security/bulle	O-GOO-ANDRO-30516/211

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
			allows physically proximate attackers to bypass the Factory Reset Protection protection mechanism and delete data via unspecified vectors, aka internal bug 26154410. **Reference** : **CVE-2016-2421**	tin/2016-04-02.html	
Bypass	17-April-2016	5.8	The PORCHE_PAIRING_CONFLICT feature in Bluetooth in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 allows remote attackers to bypass intended pairing restrictions via a crafted device, aka internal bug 26551752. **Reference** : **CVE-2016-0850**	https://android.googlesource.com/platform/external/bluetooth/bluedroid/+/c677ee92595335233eb0e7b59809a1a94e7a678a	O-GOO-ANDRO-30516/212
Bypass	17-April-2016	7.2	Race condition in Download Manager in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 allows attackers to bypass private-storage file-access restrictions via a crafted application that changes a symlink target, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26211054.	https://android.googlesource.com/platform/packages/providers/DownloadProvider/+/bdc831357e7a116bc561d51bf2ddc85ff11c01a9	O-GOO-ANDRO-30516/213

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference : **CVE-2016-0848**		
Bypass;Gain Information	17-April-2016	10	media/libmedia/IDrm.cpp in mediaserver in Android 6.x before 2016-04-01 does not initialize a certain key-request data structure, which allows attackers to obtain sensitive information from process memory, and consequently bypass an unspecified protection mechanism, via unspecified vectors, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26323455.	https://android.googlesource.com/platform/frameworks/av/+/5a856f2092f7086aa0fea9ae06b9255befcdcd34	O-GOO-ANDRO-30516/214
			Reference : **CVE-2016-2419**		
Bypass;Gain Information	17-April-2016	10	media/libmedia/IOMX.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not initialize a parameter data structure, which allows attackers to obtain sensitive information from process memory, and consequently bypass an unspecified protection mechanism, via unspecified vectors, as demonstrated by	https://android.googlesource.com/platform/frameworks/av/+/1171e7c047bf79e7c93342bb6a812c9edd86aa84	O-GOO-ANDRO-30516/215

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			obtaining Signature or SignatureOrSystem access, aka internal bug 26914474. **Reference** : **CVE-2016-2417**		
Bypass;Gain Information	17-April-2016	10	libs/gui/BufferQueueConsumer.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not check for the android.permission.DUMP permission, which allows attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, via a dump request, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27046057. **Reference** : **CVE-2016-2416**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/216
Denial of Service	17-April-2016	7.1	server/content/SyncStorageEngine.java in SyncStorageEngine in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 mismanages certain authority data, which allows attackers to	https://android.googlesource.com/platform/frameworks/base/+/d3383d5bfab296ba3adbc121ff8a7b542bde4afb	O-GOO-ANDRO-30516/217

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			cause a denial of service (reboot loop) via a crafted application, aka internal bug 26513719. **Reference** : **CVE-2016-2424**		
Denail of Service;Execute Code; Memory Corruption	17-April-2016	10	An unspecified media codec in mediaserver in Android 6.x before 2016-04-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 26220548. **Reference** : **CVE-2016-0834**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/218
Denail of Service;Execute Code; Overflow; Memory Corruption	17-April-2016	10	The H.264 decoder in libstagefright in Android 6.x before 2016-04-01 mishandles Memory Management Control Operation (MMCO) data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 25818142. **Reference** : **CVE-2016-0842**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/219
Denail of Service;Execute Code; Overflow; Memory Corruption	17-April-2016	10	media/libmedia/mediametadataretriever.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/220

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
			mishandles cleared service binders, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 26040840. **Reference** : **CVE-2016-0841**		
Denail of Service;Execute Code; Overflow; Memory Corruption	17-April-2016	10	Multiple stack-based buffer underflows in decoder/ih264d_parse_cavlc.c in mediaserver in Android 6.x before 2016-04-01 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 26399350. **Reference** : **CVE-2016-0840**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/221
Denail of Service;Execute Code; Overflow; Memory Corruption	17-April-2016	10	post_proc/volume_listener.c in mediaserver in Android 6.x before 2016-04-01 mishandles deleted effect context, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 25753245. **Reference** : **CVE-2016-0839**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/222
Denail of	17-April-	10	Sonivox in mediaserver	https://androi	O-GOO-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Service;Execute Code; Overflow; Memory Corruption	2016		in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not check for a negative number of samples, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, related to arm-wt-22k/lib_src/eas_wtengine.c and arm-wt-22k/lib_src/eas_wtsynth.c, aka internal bug 26366256. **Reference** : **CVE-2016-0838**	d.googlesource.com/platform/external/sonivox/+/3ac044334c3ff6a61cb4238ff3ddaf17c7efcf49	ANDRO-30516/223
Denail of Service;Execute Code; Overflow; Memory Corruption	17-April-2016	10	MPEG4Extractor.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via a crafted media file, aka internal bug 27208621. **Reference** : **CVE-2016-0837**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/224
Denail of Service;Execute Code;	17-April-2016	10	Stack-based buffer overflow in	https://android.googlesour	O-GOO-ANDRO-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Overflow; Memory Corruption			decoder/impeg2d_vld.c in mediaserver in Android 6.x before 2016-04-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 25812590. **Reference** : **CVE-2016-0836**	ce.com/platform/external/libmpeg2/+/8b4ed5a23175b7ffa56eea4678db7287f825e985	30516/225
Denail of Service;Execute Code; Overflow; Memory Corruption	17-April-2016	10	decoder/impeg2d_dec_hdr.c in mediaserver in Android 6.x before 2016-04-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file that triggers a certain negative value, aka internal bug 26070014. **Reference** : **CVE-2016-0835**	https://android.googlesource.com/platform/external/libmpeg2/+/ba604d336b40fd4bde1622f64d67135bdbd61301	O-GOO-ANDRO-30516/226
Denail of Service; Memory Corruption	17-April-2016	4.9	The Minikin library in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 does not properly consider negative size values in font data, which allows remote attackers to cause a denial of service (memory corruption and reboot loop) via a crafted font, aka internal bug 26413177.	https://android.googlesource.com/platform/frameworks/minikin/+/f4785aa1947b8d22d5b19559ef1ca526d98e0e73	O-GOO-ANDRO-30516/227

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference : **CVE-2016-2414**		
Overflow; Gain Privileges	17-April-2016	7.2	Multiple integer overflows in minzip/SysUtil.c in the Recovery Procedure in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 allow attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26960931. **Reference** : **CVE-2016-0849**	https://android.googlesource.com/platform/bootable/recovery/+/28a566f7731b4cb76d2a9ba16d997ac5aeb07dad	O-GOO-ANDRO-30516/228
Overflow Bypass Gain Information	17-April-2016	10	media/libmedia/IOMX.cpp in mediaserver in Android 6.x before 2016-04-01 does not initialize certain metadata buffer pointers, which allows attackers to obtain sensitive information from process memory, and consequently bypass an unspecified protection mechanism, via unspecified vectors, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26324358. **Reference** : **CVE-2016-2418**	http://source.android.com/security/bulletin/2016-04-02.html	O-GOO-ANDRO-30516/229
NA	17-April-	7.2	The Telecom Component	http://source.	O-GOO-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
	2016		in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-04-01 allows attackers to spoof the originating telephone number of a call via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26864502. **Reference** : **CVE-2016-0847**	android.com/security/bulletin/2016-04-02.html	ANDRO-30516/230
Linux					
Linux Kernel The Linux kernel is a Unix-like computer operating system kernel					
Denial of Service	27-April-2016	4.9	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local users to cause a denial of service (memory consumption) by creating many pipes with non-default sizes. **Reference** : **CVE-2016-2847**	https://bugzilla.redhat.com/show_bug.cgi?id=1313428	O-LIN-LINUX-30516/231
Denial of Service	27-April-2016	4.7	sound/core/timer.c in the Linux kernel before 4.4.1 employs a locking approach that does not consider slave timer instances, which allows local users to cause a denial of service (race condition, use-after-free,	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.1	O-LIN-LINUX-30516/232

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			and system crash) via a crafted ioctl call. **Reference** : **CVE-2016-2547**		
Denial of Service	27-April-2016	4.7	sound/core/timer.c in the Linux kernel before 4.4.1 uses an incorrect type of mutex, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call. **Reference** : **CVE-2016-2546**	https://bugzilla.redhat.com/show_bug.cgi?id=1311564	O-LIN-LINUX-30516/233
Denial of Service	27-April-2016	4.7	The snd_timer_interrupt function in sound/core/timer.c in the Linux kernel before 4.4.1 does not properly maintain a certain linked list, which allows local users to cause a denial of service (race condition and system crash) via a crafted ioctl call. **Reference** : **CVE-2016-2545**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.1	O-LIN-LINUX-30516/234
Denial of Service	27-April-2016	4.7	Race condition in the queue_delete function in sound/core/seq/seq_queue.c in the Linux kernel before 4.4.1 allows local users to cause a denial of service (use-after-free and system crash) by making an ioctl call at a certain time. **Reference** : **CVE-2016-**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.1	O-LIN-LINUX-30516/235

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			2544		
Denial of Service	27-April-2016	4.9	Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor. **Reference** : **CVE-2016-2384**	https://github.com/torvalds/linux/commit/07d86ca93db7e5cdf4743564d98292042ec21af7	O-LIN-LINUX-30516/236
Denial of Service	27-April-2016	4.9	The aiptek_probe function in drivers/input/tablet/aiptek.c in the Linux kernel before 4.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device that lacks endpoints. **Reference** : **CVE-2015-7515**	https://bugzilla.redhat.com/show_bug.cgi?id=1285326	O-LIN-LINUX-30516/237
Denial of Service	27-April-2016	4.9	Memory leak in the cuse_channel_release function in fs/fuse/cuse.c in the Linux kernel before 4.4 allows local users to cause a denial of service (memory consumption) or possibly have unspecified other impact by opening	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=2c5816b4beccc8ba709144539f6fdd764f8fa49c	O-LIN-LINUX-30516/238

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			/dev/cuse many times. **Reference** : **CVE-2015-1339**		
Novell					
Leap;Opensuse openSUSE Leap is a brand new way of building openSUSE and is new type of hybrid Linux distribution					
Gain Information	18-April-2016	2.1	The quagga package before 0.99.23-2.6.1 in openSUSE and SUSE Linux Enterprise Server 11 SP 1 uses weak permissions for /etc/quagga, which allows local users to obtain sensitive information by reading files in the directory. **Reference** : **CVE-2016-4036**	https://bugzilla.suse.com/show_bug.cgi?id=770619	O-NOV-LEAP;-30516/239
Denail of Service;Execute Code;Overflow	18-April-2016	9.3	Heap-based buffer overflow in the gdk_pixbuf_flip function in gdk-pixbuf-scale.c in gdk-pixbuf 2.30.x allows remote attackers to cause a denial of service or possibly execute arbitrary code via a crafted BMP file. **Reference** : **CVE-2015-7552**	https://bugzilla.suse.com/show_bug.cgi?id=958963	O-NOV-OPENS-30516/240
Oracle					
Solaris Solaris is a Unix operating system originally developed by Sun Microsystems					
NA	21-April-2016	4.9	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect availability via	http://www.oracle.com/technetwork/security-	O-ORA-SOLAR-30516/241

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			vectors related to Network Configuration Service. **Reference** : **CVE-2016-3462**	advisory/cpuapr2016v3-2985753.html	
NA	21-April-2016	10	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to the PAM LDAP module. **Reference** : **CVE-2016-0693**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	O-ORA-SOLAR-30516/242
NA	21-April-2016	4	Unspecified vulnerability in Oracle Sun Solaris 10 allows local users to affect availability via vectors related to the kernel. **Reference** : **CVE-2016-0676**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	O-ORA-SOLAR-30516/243
NA	21-April-2016	5.2	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect integrity and availability via vectors related to Fwflash. **Reference** : **CVE-2016-0669**	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html	A-O-ORA-SOLAR-30516/244
XEN					
XEN hypervisor using a microkernel design, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.					
Denial of Service; Overflow; Gain Privileges	19-April-2016	7.2	Integer overflow in the x86 shadow pagetable code in Xen allows local guest OS users to cause	http://xenbits.xen.org/xsa/advisory-173.html	O-XEN-XEN-30516/245

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 denial of service (host crash) or possibly gain privileges by shadowing a superpage mapping. **Reference** : **CVE-2016-3960**		

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