Semana 25/04/2016

Semana 25/04/2016					
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info	
Mozilla-firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 46.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	30/04/2016	10.0	CVE-2016-2804	
Cisco-Webex	Untrusted search path vulnerability in Cisco WebEr Productivity Tools 2.40.5001.10012 allows local users to gain privileges via a Trojan horse cryptsp.dli, dwmapi.dli, msinga2.dli, mstrad.ali, propsys.dli, riched20.dli, rpcrtremote.dli, secur32.dli, sss.dli, or uxtheme.dli file in the current working directory. Asa Bust DCSCuy56140.	28/04/2016	7.2	CVE-2016-4349	
Microsoft-windows	Use-affer five volarisability in the Teaffeld object insplanmentation in Adole Table Player before 18.00. 288 and 19.5 and 20.5 before 20.00.228 on Visions and OS Am of Service 17.200.256 on Living Acade All before 10.00.028 days and Service 12.00.256 on Living Acade All before 10.00.00.000 and Acade All Service 10.00.000 and Acade All Service 10.00.000 and Acade All Service 10.000 and Acad	28/04/2016	93	QVE-2015-8823	
Ecava-integraxor	The HMI web server in Ecava IntegraXor before 5.0 build 4522 allows remote attackers to obtain sensitive cleartext information by sniffing the network.	21/04/2016	7.8	CVE-2016-2306	
Ecava-integraxor	SQL injection vulnerability in Ecava IntegraXor before 5.0 build 4522 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	21/04/2016	7.5	CVE-2016-2299	
Oracle-outside	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.	21/04/2016	9.0	CVE-2016-3455	
Oraclejdk	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Deployment.	21/04/2016	7.6	CVE-2016-3449	
Oraclesolaris	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows local users to affect confidentiality, integrity, and availability via vectors related to Filesystem.	21/04/2016	7.2	CVE-2016-3441	
Accuernegyacuvin	The AXM-NET module in Accuenergy Acuvim II NET Firmware 3.08 and Acuvim IIR NET Firmware 3.08 allows remote attackers to discover settings via a direct request to an unspecified URL.	21/04/2016	7.5	CVE-2016-2293	
Ciscoadaptive	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.	21/04/2016	7.8	CVE-2016-1367	
CiscoWireless	Cisco Wireless LAN Controller (WLC) Software 7.4 before 7.4.130.0(MD) and 7.5, 7.6, and 8.0 before 8.0.110.0(ED) allows remote attackers to cause a denial of service (device reload) via crafted Bonjour traffic, aka Bug ID CSCur66908.	21/04/2016	7.8.	CVE-2016-1364	
Ciscoaireos	Cisco AireOS 4.1 through 7.4.120.0, 7.5.x, and 7.6.100.0 on Wireless LAN Controller (WLC) devices allows remote attackers to cause a denial of service (device reload) via a crafted HTTP request, aka Bug ID CSCun86747.	21/04/2016	7.8	CVE-2016-1362	

	Semana 18/04/2016			
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
Oracle-mysql	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.	21/04/2016	10.0	CVE-2016-0639
Oracle-weblogic	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.	21/04/2016	<u>7.5.</u>	CVE-2016-0638
Ciscounified	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 packets, aka Bug ID CSCux00686.	21/04/2016	7.8	CVE-2015-6360
Optipng	Use-after-free vulnerability in OptiPNG 0.6.4 allows remote attackers to execute arbitrary code via a crafted PNG file.	20/04/2016	9.3	CVE-2015-7801
Suselinux	Multiple stack-based buffer overflows in the GNU C Library (aka gibb 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) nanf function.	19/04/2016	<u>7.5</u>	CVE-2014-9761
Suselinux	Stack-based buffer overflow in the catopen function in the GNU C Library (aka gilbc or lbc6) 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.	19/04/2016	7.5	CVE-2015-8779
Suselinux	Integer overflow in the GNU C Library (aka gibc 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 thehcreate_f function, which triggers out-of-bounds head-memory access.	19/04/2016	<u>7.5</u>	CVE-2015-8778
Fedoraproject	$slapd/connection.c in 389 \ Directory Server (formerly Fedora Directory Server) \ 1.3.4 x \ before \ 1.3.4.7 \ allows \ remote attackers to cause a denial of service (infinite loop and connection blocking) by leveraging an abnormally closed connection.$	19/04/2016	7.8	CVE-2016-0741
TibcoEnterprise	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.	19/04/2016	7.2	CVE-2016-3960
Pandaendpoint	Panda Endpoint Administration Agent before 7.50.00, as used in Panda Security for Business products for 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.	18/04/2016	7.2.	CVE-2016-3943
PandaSecurity	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.	18/04/2016	7.2	CVE-2015-7378
Fedoraproject	Format string vulnerability in the CmdKeywords function in funct1.c in latex2rtf before 2.3.10 allows remote attackers to execute arbitrary code via format string specifiers in the \keywords command in a crafted TeX file.	18/04/2016	9.3	CVE-2015-8106
Novellopensuse	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.	18/04/2016	9.3	CVE-2015-7552
Googlechrome	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.	18/04/2016	10.0	CVE-2016-1659
Googlechrome	Google Chrome before \$0.0.2661.75 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 unspecified other impact via a crafted extension.	18/04/2016	7.5	CVE-2016-1655
Googlechrome	The LoadBuffer implementation in Google VR, as used in Google Chrome before 50.0.2661.75, 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 wire operation, related to complete/pipeline.cr and compiler/pipeline-dowering cr.	18/04/2016	9.3	CVE-2016-1653
Googleandroid	dhopd before 6.100, as used in Android 4.x before 4.4.4, 5.0x before 5.0.2, 5.1x 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 Z6461634.	17/04/2016	10.0	CVE-2016-1503
Googleandroid	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.	17/04/2016	9.3	CVE-2016-2420
Googleandroid	media/Tibmedia/TOMX.cpp in mediaserver in Android 6.x before 2016-04-01 does not initialize certain metadata buffer pointers, which advantages trackers to obtain sensible information from process memory, and consequently bypass an unspecified protection mechanism, via unspecified vectors, as demonstrated by obtaining Signature or Signature-Originate maces, ski internal bug 26224358.	17/04/2016	10.0	CVE-2016-2418
Googleandroid	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, akia internal bug 26488455.	17/04/2016	<u>7.1</u>	CVE-2016-2415
Googleandroid	media/libmedia/O/DMX.cpp in mediaserver in Android 5.0.x before 5.02, 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 Signature/Orsystem access, aka internal bug 2640/3627.	17/04/2016	9.3	CVE-2016-2413
Googleandroid	include/core/SAPostConfig h in Skia, as used in System_server in Android 4.x before 4.4.4, S.0.x before 5.0.2, S.1.x before 5.1.1, and 6.x before 2016-04-01, mishandles certain crashes, which allows attacker to gain privilege: via a crafted application, as demonstrated by obtaining Squature or Signature/Objectma excess, skal anternal bug 25059390.	17/04/2016	9.3	CVE-2016-2412
Googleandroid	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.	17/04/2016	9.3	CVE-2016-2411
Googleandroid	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.	17/04/2016	9.3	CVE-2016-2409
Googleandroid	Multiple integer overflows in minzip/SysUtil.c in the Recovery Procedure in Android 5.0x 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 Signature Orseivem access a kin internal bus 25960-013.	17/04/2016	7.2	CVE-2016-0849
Googleandroid	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 slows attaken to bypass private-storage file-acces restrictions via a crafted application that changes a symilink target, as demonstrated by absolating Signature or Signature Originature cases, ask internal by 26211054.	17/04/2016	7.2	CVE-2016-0848
Googleandroid	The Telecom Component 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, ski others In the 78645470?	17/04/2016	7.2	CVE-2016-0847
Googleandroid	lbs/binder/Memory.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 2.016-04-01 does not properly consider the heap size, which allows attackers to gain privileges via a crafted application, as demonstrated by bottaining Signature or Signature/Orighten access, ska internal bug 26877992.	17/04/2016	7.2	CVE-2016-0846
Googleandroid	The Qualcomm RF driver in Android 6.x before 2016-04-01 does not properly restrict access to socket ioctl calls, which allows attackers to gain privileges via a crafted application, aka internal bug 26324307.	17/04/2016	7.2	CVE-2016-0844
Googleandroid	The Qualcomm ARM processor performance-event manager in Android $4x$ before $4.44$ , $5.0x$ before $5.0.2$ , $5.1x$ before $5.1.1$ , and $6x$ before $2016-04-01$ allows attackers to gain privileges via a crafted application, aka internal bug 25801197.	17/04/2016	7.2	CVE-2016-0843
Googleandroid	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 bus 25818142.	17/04/2016	10.0	CVE-2016-0842
Googleandroid	media/libmedia/mediametadataretriever.cpp in mediaserver in Android 4x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6x before 2016-04-01 mishandies cleared service binders, which allows remote attackers to execute arbitrary code or cause a denial of service immore corruption) via a cardior media file, six internal bug 2500/800.	17/04/2016	10.0	CVE-2016-0841
Googleandroid	Multiple stack-based buffer underflows in decoder/in/264d_parse_cavk.c in mediaserver in Android 6.x before 2016-04-01 allow remote stackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 26399350.	17/04/2016	10.0	CVE-2016-0840
Googleandroid	Constraint, or the control of the co	17/04/2016	10.0	CVF-2016-0839
Googleandroid	Seriorio is mediasenver in deriorio 4.a before 4.4.4, 5.0 before 5.0.2, 5.1 before 5.1.1, and 6.a before 2016-04-01 does not check for a negative inventor of samples, which allows remote attackers to secutive attrizance doer or case a deviated of service (memory compition) via a carifed media file, related to arm-wt-224/lb_src/eas_whrengine.c and arm-wt-224/lb_src/eas_whynth.c, aka internal law 23660556	17/04/2016	10.0	CVE-2016-0838
Googleandroid	2002 d'8044206. MPGG44traction: cpp in libitagefright 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 2016-0-6.1 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory correspion) via a cartied media file, ask internal bug 2720804.	17/04/2016	10.0	CVE-2016-0837
Googleandroid	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.	17/04/2016	10.0	CVE-2016-0835
Googleandroid	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.	17/04/2016	10.0	CVE-2016-0834

Primary Vendor Product	Semana 11/04/2016	Published	CVSS Score	Source & Patch Info
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Into
Googleandroid	Stack-based buffer overflow in 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.	17/04/2016	10.0	CVE-2016-0836
Ciscounified	Heap-based buffer overflow in Cisco Unified Computing System (UCS) Platform Emulator 2.5(2)TS4, 3.0(2c)A, and 3.0(2c)TS9 allows local users to gain privileges via crafted libclimeta.so filename arguments. aka Buz ID CSCux68837.	15/04/2016	<u>7.2</u>	CVE-2016-1340
Ciscounified	Cisco Unified Computing System (UCS) Platform Emulator 2.5(2)TS4, 3.0(2c)A, and 3.0(2c)TS9 allows local users to gain privileges via crafted arguments on a ucspe-copy command line. aka Bug ID CSCux68832.	15/04/2016	<u>7.2</u>	CVE-2016-1339
Juniper-screenos	The administrative web services interface in Juniper ScreenOS before 6.3.0r21 allows remote attackers to cause a denial of service frebooth via a crafted SSL packet.	15/04/2016	7.8	CVE-2016-1268
Sapnetweaver	XML external entity (XXE) vulnerability in the UDDI component in SAP NetWeaver JAVA AS 7.4 allows remote attackers to cause a denial of service via a crafted XML request, aka SAP Security Note 2254389.	14/04/2016	9.0	CVE-2016-4014
Apachesubersion	Integer overflow in util.c in mod_dar_svn in Apache Subversion 1.7.x, 1.8.x before 1.8.15, and 1.9.x before 1.9.3 allows remote authenticated users to cause a definial of service (subversion server crash or memory consumption) and possibly execute arbitrary code use a sket-encoded request body, which regiges and out-forwords read and heap-based buffer overflequest body. Which regiges no user of bounds read and heap-based buffer overflequest body.	14/04/2016	8.0	CVE-2015-5343
Debian-linux	Meap-based buffer overflow in the bmp_read_rows function in pngxrbmp.c in OptiPNG before 0.7.6 allows remote attackers to cause a denial of service (out-of-bounds read or write access and crash) or possibly execute arbitrary code via a crafted image file.	13/04/2016	9.3	CVE-2016-3981
Huawei-mate	Integer overflow in the graphics drivers in Huawel Mate S smartphones with software CRR-TL00 before CRR-TL0001B16GSP01, CRR- LL00 before CRR-LL00000B160, and CRR-L00 before CRR-L00052B163 allows attackers to cause a denial of service (system crash) or gain privileges vs a carted application, which trigges a heap-based buffer overflow.	13/04/2016	9.3	CVE-2016-1495
Avast-freeantivirus	Meap-based buffer overflow in the Avast virtualization driver (aswSnx.sys) in Avast Internet Security, Pro Antivirus, Premier, and Free Antivirus before 11.1.2253 allows local users to gain privileges via a Unicode file path in an IOCTL request.	13/04/2016	10.0	CVE-2015-8620
Huawei-P7	Integer overflow in Huawei P7 phones with software before P7-L07 V100R001C01B606 allows remote attackers to gain privileges via a crafted annitration with the system or camera nermission.	13/04/2016	9.3	CVE-2015-8304
Microsoftwindows	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and RZ SP1, Windows 7 SP1, Windows 8.1, Windows 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, also Visual's Elevation of Privilege Visinerability, and Referent winerability fant OVE-2015-0613 and CVE-2016-06106.	12/04/2016	7.2	CVE-2016-0167
Microsoftintenetexplorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	12/04/2016	7.6	CVE-2016-0166
Microsoftwindows	The kernet-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1. Windows Server 2012 Gold and R31, Windows 10 and Last and Windows 10 and Last and Last Revision of Privilege was a crafted application, sat Windows 10 and Last Revision of Privilege Vision Annies, a different volentiability than CVE 2016-1014 and CVE 2016-0107.	12/04/2016	7.2.	CVE-2016-0165
Microsoftintenetexplorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	12/04/2016	<u>7.6</u>	CVE-2016-0164
Microsoftintenetexplorer	Microsoft Internet Explorer 11 mishandles DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability."	12/04/2016	7.2	CVE-2016-0160
Microsoftintenetexplorer	Microsoft Internet Explorer 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	12/04/2016	.7.6	CVE-2016-0159
Microsoftedge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0156.	12/04/2016	<u>7.6</u>	CVE-2016-0157
Microsoftedge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different wulnerability than CVE-2016-0155 and CVE-2016-0157.	12/04/2016	7.6	CVE-2016-0156
Microsoftedge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vuinerability," a different vuinerability than CVE-2016-0156 and CVE-2016-0157.	12/04/2016	<u>7.6</u>	CVE-2016-0155
Microsoftedge	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	12/04/2016	<u>7.6</u>	CVE-2016-0154
Microsoftwindows	OLE in Microoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows R1, Windows Server 2012 Gold and R2, and Windows RT 8.1 allows remote attackers to execute arbitrary code via a crafted file, aka "Windows OLE Remote Code Execution Vulmerability."	12/04/2016	9.3	CVE-2016-0153
Microsoftwindows	The Client-Server Run-time Subsystem (CSRSS) in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT.8.1, and Windows 10 Gold and 1511 mismanages process tokens, which allows local users to gain privileges via a crafted application, alsa "Windows CSRSS-Security Feature Bypass Vulnerability."	12/04/2016	7.2	CVE-2016-0151
Microsoftwindows	HTTP-sys in Microsoft Windows 10 Gold and 1511 allows remote attackers to cause a denial of service (system hang) via crafted HTTP 2.0 requests, aka "HTTP-sys Denial of Service Vulnerability."	12/04/2016	<u>7.8</u>	CVE-2016-0150
Microsoftnetframework	Microsoft .NET Framework 4.6 and 4.6.1 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ".NET Framework Remote Code Execution Vulnerability."	12/04/2016	7.2	CVE-2016-0148
Microsoftxml	Microsoft XML Core Services 3.0 allows remote attackers to execute arbitrary code via a crafted web site, aka "MSXML 3.0 Remote Code Execution Vulnerability."	12/04/2016	9.3	CVE-2016-0147
Microsoftlive	The font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1; Windows 8.1, Windows 8.1, Windows 8.2, Windows 8.1, Windows 8	12/04/2016	9.3	CVE-2016-0145
Microsoftwindows	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows 18 A1, and Windows 10 Gold and 15.11 allows local users to gain privileges via a crafted application, kai "Window Elevation of Privilege Visionability", a different visionality than CVE_2016 GlS and CVE_	12/04/2016	7.2	CVE-2016-0143
Microsoftexcel	Microsoft Excel 2010 SP2, Word for Mac 2011, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office	12/04/2016	9.3	CVE-2016-0139
Microsoftsharepoint	document, aka "Microsoft Office Memory Corruption Vulnerability."  Microsoft Excel 2007 593, Excel 2010 592, Office Compatibility Pack 593, Excel Services on SharePoint Server 2007 593, and Excel Services on SharePoint Server 2010 592 alliow remote attackers to execute arbitrary code via a crafted Office document, aka	12/04/2016	9.3	CVE-2016-0136
Microsoftwindows	"Microsoft Office Memory Corruption Vulnerability."  The Secondary Logon Service in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka	12/04/2016	7.2	CVE-2016-0135
Microsoftoffice	"Secondary Lagon: lievation of Privilege Vulnerability."  Microsoft Word 2007 59, Office 2010 592, Word 2010 592, Word 2013 594, Word 2013 8754, Office Compatibility Pack SP3, Word  Microsoft Word 2007 593, Office 2010 592, Word Automation Services on SharePoint Server 2013 594, Office  Word Apps 2010 592, and Office Web Apps Server 2013 591 allow remote attackers to execute arbitrary code via a crafted Office  document, also "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0127
Microsoftexcel	Microsoft Excel 2007 5P3, Excel 2010 5P2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Word 2016 for Mac, Office Compatibility Pack 5P3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corrustion Vulnerability."	12/04/2016	9.3	CVE-2016-0122
Huawei-policy	Extrapour vourierability.  Huawei Policy Center with software before V100R003C10SPC020 allows remote authenticated users to gain privileges and cause a denial of service (system crash) via a crafted URL.	12/04/2016	9.0	CVE-2016-2405
Apachestruts	genial or service (system crash) via a cratted usc.  Apache Struts 2.x before 2.3.28 allows remote attackers to execute arbitrary code via a "%()" sequence in a tag attribute, aka forced drabble OGMI evaluation.	12/04/2016	10.0	CVE-2016-0785
Microsoftwindows	double COUNT. evaluation.  The Escape interface in the Kernel Mode Driver layer in the NVIDIA GPU graphics driver R340 before 341.95 and R352 before 354.74 on Windows improperly allows access to restricted functionality, which allows local users to gain privileges via unspecified vectors.	12/04/2016	7.2	CVE-2016-2556
Avast	Avast allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via a crafted PE	11/04/2016	9.3	CVE-2016-3986
	file, related to authenticode parsing.  Use-after-free vulnerability in hw/ide/ahci.c in QEMU, when built with IDE AHCI Emulation support, allows guest OS users to cause a	11/04/2016		
Qemu Claws-mail	denial of service (instance crash) or possibly execute arbitrary code via an invalid AHCI Native Command Queuing (NCQ) AIO command.  Stack-based buffer overflow in the conv_euctojis function in codeconv.c in Claws Mail 3.13.1 allows remote attackers to have		9.3	CVE-2016-1568
	unspecified impact via a crafted email, involving Japanese character set conversion. NOTE: this vulnerability exists because of an incomplete fit of CV-2-015-8614.  The CSV export in Apache LDAP Studio and Apache Directory Studio before 2.0.0-Ms10 does not properly escape field values, which	11/04/2016	7.5	CVE-2015-8708
Apachedirectory	might allow attackers to execute arbitrary commands by leveraging a crafted LDAP entry that is interpreted as a formula when imported into a poredaheet.  The TripleO Heat templates (tripleo-heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 7.0, do not properly use	,-,	9.3	CVE-2015-5349
Redhatopenstacks	the configured RabbitMQ credentials, which makes it easier for remote attackers to obtain access to services in deployed overclouds by leveragine knowledge of the default credentials. Lenovo Fingerprint Manager before 8.01.57 and Touch Fingerprint before 1.00.08 use weak ACLs for unspecified (1) services and (2)	11/04/2016	7.5	CVE-2015-5329
Lenovofingerprint	Lenovo Fingerprint Manager before 8.01.57 and Touch Fingerprint before 1.00.08 use weak ACLs for unspecified (1) services and (2) files, which allows local users to gain privileges by invalidating local checks.	11/04/2016	<u>7.2</u>	CVE-2016-2393

	Published		Source & Patch Info	
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
Adobeflash player	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OSX and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via crafted JPEG-XR data.	08/04/2016	9.3	CVE-2016-1018
Adobeflash player	Use after-free vulnerability in the LoadVars. decode function in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and GX and before 11.2.0.216 flo on lineal datows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CV-2:016-101, CV-2:016-1018, CV-2:016-1018, and CV-2:016-1018.	08/04/2016	9.3	CVE-2016-1017
Microsoftwindows10	Use after-free valuerability in the Transform object implementation in Adobe Flash Player before 18.00.343 and 19.x through 21.x before 21.00.213 on Windows and OS X and before 11.200.2616 on Linux allows attackers to execute arbitrary code via a flash geom. Matter callabod, a different valuerability hand VC-206-1011, VC-206-1013, VC-206-1037, and VC-206-1013.	08/04/2016	9.3	CVE-2016-1016
Microsoftwindows8,1	Untrusted search path vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows local users to gain privileges via a Trojan horse resource in an unspecified directory.	08/04/2016	7.2	CVE-2016-1014
Rubyonrailsruby	Action Pack in Ruby on Rails before 3.2.22.2, 4.x before 4.1.14.2, and 4.2.x before 4.2.5.2 allows remote attackers to execute arbitrary Ruby code by leveraging an application's unrestricted use of the render method.	07/04/2016	<u>7.5</u>	CVE-2016-2098
cloudbeesjetkins	Multiple unspecified API endpoints in CloudBees Jenkins before 1.650 and LTS before 1.642.2 allow remote authenticated users to execute arbitrary code via serialized data in an XML file, related to XStream and groovy.util.Expando.	07/04/2016	9.0	CVE-2016-0792
Huaweimate	The oxing driver in Hausen Fill smartphones with software GRA-TLOD before GRA-TLOCOSIB230, GRA-TLOCOSIB230, GRA-TLOCOSIB230, GRA-TLOCOSIB230, GRA-TLOCOSIB230, GRA-TLOCOSIB230, and Mate S insurphones with software CRA-TLOCOSIB230, and GRA-TLOCOSIB230, and GRA-TL	07/04/2016	9.3	CVE-2015-8681
Huaweip8	The Corplice driver in Hazawe file Smartphones with software CBA-TLOD before GBA-TLODC018230, GBA-CLOD before GBA- CLODC038230, GBA-CLID before GBA-CLIDC038230, GBA-ULID before GBA-ULID CO008230, and GBA-ULID before GBA-ULID CO08230, and GBA-ULID before CBA-ULID before	07/04/2016	9.3	CVE-2015-8680
Huaweimate	Neap-based buffer overflow in the MRI driver in Huawei P8 smartphones with software GRA-TLID before GRA-TLIDC018220, GRA- CLID before GRA-CLIDC522230, GRA-CLID before GRA-CLIDC522230, GRA-LIDD before GRA-UDC002230, and GRA-ULID before GRA-ULIC0002230, and MAter Samartphone with onbraver GRA-IDD before GRA-UDC002230, GRA-UDC002230, and GRA-UDC002230, and GRA-UDC002230, and GRA-UDC002230, and GRA-UDC002230, and GRA-UDC0022300, and GRA-UDC00223000, and GRA-UDC0022300, and GRA-UDC00223	07/04/2016	9.3	CVE-2015-8319

Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
Huaweimate	Heap-based buffer overflow in the HRI driver in Huawei R9 smartphones with software GRA-TLO0 before GRA-TL000E18230, GRA-LO10 before GRA-CL00E28230, GRA-LO10 before GRA-CL00E28230, GRA-LO10E28230, GRA-LO10E	07/04/2016	9.3	CVE-2015-8318
Huaweimate	The Graphics driver in Huawei P8 smartphones with software GBA-TL00 before GBA-TL00C018230, GBA-CL00 before GBA-L00C018230, GBA-CL00 before GBA-L00C08230, and GBA-L10 before CBA-L00C08230, and GBA-L10 before CBA-L00C082300, and GBA-L10 before CBA-L00C08300, and CBA-L10 before CBA-L00C08300, and CBA-L00 before CBA-L00C08300, and CBA-L00C082300, and	07/04/2016	9.3	CVE-2015-8307
Sap-netweaver	XML external entity (IXE) vulnerability in the Configuration Wizard in SAP NetWeaver Java AS 7.4 allows remote attackers to cause a denial of service, conduct SMB Relay attacks, or access arbitrary files via a crafted XML request, related to the ctcprotocol serviet, aka SAP Security Note 2235994.	07/04/2016	7.5	CVE-2016-3974
Squidcache	Heap-based buffer overflow in the kmp6::Recv function in icmp/kmp6.cc in the pinger in Squid before 3.5.16 and 4.x before 4.0.8 allows remote servers to cause a denial of service (performance degradation or transition failures) or write sensitive information to log files via an ICMP% packet.	07/04/2016	7.5	CVE-2016-3947
Adobeflashplayer	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors, as exploited in the wild in April 2016.	07/04/2016	10.0	CVE-2016-1019
Emcdocumentum	EMC Documentum D2 before 4.6 lacks intended ACLs for configuration objects, which allows remote authenticated users to modify objects via unspecified vectors.	07/04/2016	9.0	CVE-2016-0888
Ciscotelepresence	The kernel in Cisco TelePresence Server 3.0 through 4.2(4.18) on Mobility Services Engine (MSE) 8710 devices allows remote attackers to cause a denial of service (panic and reboot) via a crafted sequence of IPv6 packets, aka Bug ID CSCuu46673.	06/04/2016	7.1	CVE-2016-1346
Ciscoucs	Cisco UCS Invicta C3124SA Appliance 4.3.1 through 5.0.1, UCS Invicta Scaling System and Appliance, and Whiptail Racerunner improperly store a default SSH private key, which allows remote attackers to obtain root access via unspecified vectors, aka Bug ID CSCun71294.	06/04/2016	10.0	CVE-2016-1313
Ciscoevolved	Cisco Prime Infrastructure 1.2.0 through 2.2(2) and Cisco Evolved Programmable Network Manager (EPNM) 1.2 allow remote attackers to execute arbitrary code via crafted deserialized data in an HTTP POST request, aka Bug ID CSCuw03192.	06/04/2016	9.3	CVE-2016-1291
Ciscotelepresence	Gsco TelePresence Server 4.1(2.29) through 4.2(4.17) on 7010; Mobility Services Engine (MSE) 8710; Multiparty Media 310, 320, and 820; and Virtual Muchine (VM) devices allows renote attackers to cause a denial of service (memory consumption or device reload) via cartled HTP requests that are not followed by an unspecified negolation, ask alog DCCsw07550.	06/04/2016	7.8	CVE-2015-6313
Ciscotelepresence	Cisco TelePresence Server 3.1 on 7010, Mobility Services Engine (MSE) 8710, Multiparty Media 310 and 320, and Virtual Machine (VM) devices allows remote attackers to cause a denial of service (device reload) via malformed STUN packets, aka Bug ID CSCuv01348.	06/04/2016	7.8.	CVE-2015-6312
Fedoraproject	The mod_lts module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.	05/04/2016	10.0	CVE-2016-3125
Hp-asset	HPE Asset Manager 9.40, 9.41, and 9.50 and Asset Manager CloudSystem Chargeback 9.40 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	05/04/2016	<u>7.5.</u>	CVE-2016-2000
Ibm-tivoli	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8520, and CVE-2015-8521.	05/04/2016	<u>7.5</u>	CVE-2015-8522
Ibm-tivoli	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.1.2.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8520, and CVE-2015-8522.	05/04/2016	<u>7.5.</u>	CVE-2015-8521
Ibm-tivoli	Buffer overflow in the server in IBM Twoil Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8521, and CVE-2015-8522.	05/04/2016	<u>7.5</u>	CVE-2015-8520
Ibm-tivoli	Buffer overflow in the server in IBM Twoil Storage Manager FastBack 5.5.x and 6.x before 6.1.1.2.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8520, CVE-2015-8521, and CVE-2015-8522.	05/04/2016	7.5	CVE-2015-8519
Pattersondental	Patterson Dental Eaglesoft 17 has a hardcoded password of sql for the dba account, which allows remote attackers to obtain sensitive Dental DB patient information via SQL statements.	01/04/2016	10.0	CVE-2016-2343