Histórico de vulnerabilidades de Abril del 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 WebEx Productivity Tools 2.40.5001.10012 allows local users to gain privileges via a Trojan horse cryptsp.dll, dwmapi.dll, msimg32.dll, ntmarta.dll, propsys.dll, riched20.dll, rpcrtremote.dll, secur32.dll, sxs.dll, or uxtheme.dll file in the current working directory, aka Bug ID CSCuy56140.	28/04/2016	7.2	CVE-2016-4349
Microsoft-windows	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted text property, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, CVE-2015-8821, and CVE-2015-8822.	28/04/2016	9.3	CVE-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
Oracle--jdk	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
Oracle--solaris	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
Accuernegy--acuvin	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
Cisco--adaptive	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
Cisco--Wireless	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
Cisco--aireos	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	7.5	CVE-2016-0638
Cisco--unified	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
Suse--linux	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.	19/04/2016	7.5	CVE-2014-9761
Suse--linux	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.	19/04/2016	7.5	CVE-2015-8779
Suse--linux	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.	19/04/2016	7.5	CVE-2015-8778
Fedora--project	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
Tibco--Enterprise	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
Panda--endpoint	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
Panda--Security	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
Fedora--project	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
Novell--opensuse	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
Google--chrome	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
Google--chrome	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 unspecified other impact via a crafted extension.	18/04/2016	7.5	CVE-2016-1655
Google--chrome	The LoadBuffer implementation in Google V8, 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 write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc.	18/04/2016	9.3	CVE-2016-1653
Google--android	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.	17/04/2016	10.0	CVE-2016-1503
Google--android	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
Google--android	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.	17/04/2016	10.0	CVE-2016-2418
Google--android	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.	17/04/2016	7.1	CVE-2016-2415
Google--android	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.	17/04/2016	9.3	CVE-2016-2413
Google--android	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.	17/04/2016	9.3	CVE-2016-2412
Google--android	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
Google--android	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
Google--android	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.	17/04/2016	7.2	CVE-2016-0849
Google--android	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.	17/04/2016	7.2	CVE-2016-0848
Google--android	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, aka internal bug 26864502.	17/04/2016	7.2	CVE-2016-0847
Google--android	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.	17/04/2016	7.2	CVE-2016-0846
Google--android	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
Google--android	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.	17/04/2016	7.2	CVE-2016-0843
Google--android	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.	17/04/2016	10.0	CVE-2016-0842
Google--android	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 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.	17/04/2016	10.0	CVE-2016-0841
Google--android	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.	17/04/2016	10.0	CVE-2016-0840
Google--android	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.	17/04/2016	10.0	CVE-2016-0839
Google--android	Sonivox 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 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.	17/04/2016	10.0	CVE-2016-0838
Google--android	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.	17/04/2016	10.0	CVE-2016-0837
Google--android	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
Google--android	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

Semana 11/04/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Google--android	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
Cisco--unified	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 Bug ID CSCux68837.	15/04/2016	7.2	CVE-2016-1340
Cisco--unified	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	7.2	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 (reboot) via a crafted SSL packet.	15/04/2016	7.8	CVE-2016-1268
Sap--netweaver	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
Apache--subersion	Integer overflow in util.c in mod_dav_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 denial of service (subversion server crash or memory consumption) and possibly execute arbitrary code via a skel-encoded request body, which triggers an out-of-bounds read and heap-based buffer overflow.	14/04/2016	8.0	CVE-2015-5343
Debian-linux	Heap-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 Huawei Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, which triggers a heap-based buffer overflow.	13/04/2016	9.3	CVE-2016-1495
Avast-freeantivirus	Heap-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 application with the system or camera permission.	13/04/2016	9.3	CVE-2015-8304
Microsoft--windows	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 RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0143 and CVE-2016-0165.	12/04/2016	7.2	CVE-2016-0167
Microsoft--intenetexplorer	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
Microsoft--windows	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 RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0143 and CVE-2016-0167.	12/04/2016	7.2	CVE-2016-0165
Microsoft--intenetexplorer	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	7.6	CVE-2016-0164
Microsoft--intenetexplorer	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
Microsoft--intenetexplorer	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
Microsoft--edge	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	7.6	CVE-2016-0157
Microsoft--edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0157.	12/04/2016	7.6	CVE-2016-0156
Microsoft--edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0156 and CVE-2016-0157.	12/04/2016	7.6	CVE-2016-0155
Microsoft--edge	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	7.6	CVE-2016-0154
Microsoft--windows	OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, 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 Vulnerability."	12/04/2016	9.3	CVE-2016-0153
Microsoft--windows	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, aka "Windows CSRSS Security Feature Bypass Vulnerability."	12/04/2016	7.2	CVE-2016-0151
Microsoft--windows	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	7.8	CVE-2016-0150
Microsoft--netframework	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
Microsoft--xml	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
Microsoft--live	The font library 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 RT 8.1; Windows 10 Gold and 1511; Office 2007 SP3 and 2010 SP2; Word Viewer; .NET Framework 3.0 SP2, 3.5, and 3.5.1; Skype for Business 2016; Lync 2010; Lync 2010 Attendee; Lync 2013 SP1; and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0145
Microsoft--windows	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 RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0165 and CVE-2016-0167.	12/04/2016	7.2	CVE-2016-0143
Microsoft--excel	Microsoft Excel 2010 SP2, Word for Mac 2011, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0139
Microsoft--sharepoint	Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0136
Microsoft--windows	The Secondary Logon Service in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Secondary Logon Elevation of Privilege Vulnerability."	12/04/2016	7.2	CVE-2016-0135
Microsoft--office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0127
Microsoft--excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Word 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0122
Huawei-policy	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
Apache--struts	Apache Struts 2.x before 2.3.28 allows remote attackers to execute arbitrary code via a "%{}" sequence in a tag attribute, aka forced double OGNL evaluation.	12/04/2016	10.0	CVE-2016-0785
Microsoft--windows	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 file, related to authenticode parsing.	11/04/2016	9.3	CVE-2016-3986
Qemu	Use-after-free vulnerability in hw/ide/ahci.c in QEMU, when built with IDE AHCI Emulation support, allows guest OS users to cause a denial of service (instance crash) or possibly execute arbitrary code via an invalid AHCI Native Command Queuing (NCQ) AIO command.	11/04/2016	9.3	CVE-2016-1568
Claws--mail	Stack-based buffer overflow in the conv_euctojis function in codeconv.c in Claws Mail 3.13.1 allows remote attackers to have unspecified impact via a crafted email, involving Japanese character set conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8614.	11/04/2016	7.5	CVE-2015-8708
Apache--directory	The CSV export in Apache LDAP Studio and Apache Directory Studio before 2.0.0-M10 does not properly escape field values, which might allow attackers to execute arbitrary commands by leveraging a crafted LDAP entry that is interpreted as a formula when imported into a spreadsheet.	11/04/2016	9.3	CVE-2015-5349
Redhat--openstacks	The TripleO Heat templates (tripleo-heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 7.0, do not properly use the configured RabbitMQ credentials, which makes it easier for remote attackers to obtain access to services in deployed overclouds by leveraging knowledge of the default credentials.	11/04/2016	7.5	CVE-2015-5329
Lenovo--fingerprint	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	7.2	CVE-2016-2393

Semana 04/04/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--flash 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 OS X 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
Adobe--flash 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 OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1031.	08/04/2016	9.3	CVE-2016-1017
Microsoft--windows10	Use-after-free vulnerability in the Transform object implementation 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 attackers to execute arbitrary code via a flash.geom.Matrix callback, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1017, and CVE-2016-1031.	08/04/2016	9.3	CVE-2016-1016
Microsoft--windows8,1	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
Rubyonrails--ruby	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	7.5	CVE-2016-2098
cloudbees--jetkins	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
Huawei--mate	The ovisp driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-CL10 before GRA-CL10C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230, and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application with the camera permission, aka an "interface access control vulnerability."	07/04/2016	9.3	CVE-2015-8681
Huawei--p8	The Graphics driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-CL10 before GRA-CL10C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230, and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application with the graphics permission, aka an "interface access control vulnerability," a different vulnerability than CVE-2015-8307.	07/04/2016	9.3	CVE-2015-8680
Huawei--mate	Heap-based buffer overflow in the HIFI driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-CL10 before GRA-CL10C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230, and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2015-8318.	07/04/2016	9.3	CVE-2015-8319

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Huawei--mate	Heap-based buffer overflow in the HIFI driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-CL10 before GRA-CL10C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230, and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2015-8319.	07/04/2016	9.3	CVE-2015-8318
Huawei--mate	The Graphics driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-CL10 before GRA-CL10C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230, and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application with the graphics permission, aka an "interface access control vulnerability," a different vulnerability than CVE-2015-8680.	07/04/2016	9.3	CVE-2015-8307
Sap-netweaver	XML external entity (XXE) vulnerability in the Configuration Wizard in SAP NetWeaver Java AS 7.4 allows remote attackers to cause a denial of service, conduct SMB Relay attacks, or access arbitrary files via a crafted XML request, related to the ctcprotocol servlet, aka SAP Security Note 2235994.	07/04/2016	7.5	CVE-2016-3974
Squid--cache	Heap-based buffer overflow in the Icmp6::Recv function in icmp/Icmp6.cc in the pinger in Squid before 3.5.16 and 4.x before 4.0.8 allows remote servers to cause a denial of service (performance degradation or transition failures) or write sensitive information to log files via an ICMPv6 packet.	07/04/2016	7.5	CVE-2016-3947
Adobe--flashplayer	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
Emc--documentum	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
Cisco--telepresence	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
Cisco--ucs	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
Cisco--evolved	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
Cisco--telepresence	Cisco 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 Machine (VM) devices allows remote attackers to cause a denial of service (memory consumption or device reload) via crafted HTTP requests that are not followed by an unspecified negotiation, aka Bug ID CSCuv47565.	06/04/2016	7.8	CVE-2015-6313
Cisco--telepresence	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
Fedora--project	The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a 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	7.5	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	7.5	CVE-2015-8522
Ibm-tivoli	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8520, and CVE-2015-8522.	05/04/2016	7.5	CVE-2015-8521
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-2015-8521, and CVE-2015-8522.	05/04/2016	7.5	CVE-2015-8520
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-2015-8520, CVE-2015-8521, and CVE-2015-8522.	05/04/2016	7.5	CVE-2015-8519
Patterson--dental	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