Histórico de vulnerabilidades de Enero del 2016

Semana 25/01/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lexmark -- printer_firmware	Race condition in the initialization process on Lexmark printers with firmware ATL before ATL.02.049, CB before CB.02.049, PP before PP.02.049, and YK before YK.02.049 allows remote attackers to bypass authentication by leveraging incorrect detection of the security-jumper status.	27/01/2016	10.0	CVE-2016-1896
debian -- fuse	An unspecified udev rule in the Debian fuse package in jessie before 2.9.3-15+deb8u2, in stretch before 2.9.5-1, and in sid before 2.9.5-1 sets world-writable permissions for the /dev/cuse character device, which allows local users to gain privileges via a character device in /dev, related to an ioctl.	26/01/2016	7.2	CVE-2016-1233
microsys -- promotic	Heap-based buffer overflow in MICROSYS PROMOTIC before 8.3.11 allows remote authenticated users to cause a denial of service via a malformed HTML document.	26/01/2016	7.1	CVE-2016-0869
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 48.0.2564.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	25/01/2016	9.3	CVE-2016-1620
google -- chrome	Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	25/01/2016	7.5	CVE-2016-2052
cisco -- modular_encoding_platform_d9036_software	Cisco Modular Encoding Platform D9036 Software before 02.04.70 has hardcoded (1) root and (2) guest passwords, which makes it easier for remote attackers to obtain access via an SSH session, aka Bug ID CSCut88070.	22/01/2016	10.0	CVE-2015-6412
cisco -- unified_computing_system	An unspecified CGI script in Cisco FX-OS before 1.1.2 on Firepower 9000 devices and Cisco Unified Computing System (UCS) Manager before 2.2(4b), 2.2(5) before 2.2(5a), and 3.0 before 3.0(2e) allows remote attackers to execute arbitrary shell commands via a crafted HTTP request, aka Bug ID CSCur90888.	22/01/2016	10.0	CVE-2015-6435
harman -- amx_firmware	The setUpSubtleUserAccount function in /bin/bw on Harman AMX devices before 2015-10-12 has a hardcoded password for the BlackWidow account, which makes it easier for remote attackers to obtain access via a (1) SSH or (2) HTTP session, a different vulnerability than CVE-2016-1984.	22/01/2016	10.0	CVE-2015-8362
harman -- amx_firmware	The setUpSubtleUserAccount function in /bin/bw on Harman AMX devices before 2016-01-20 has a hardcoded password for the 1MB@tMaN account, which makes it easier for remote attackers to obtain access via a (1) SSH or (2) HTTP session, a different vulnerability than CVE-2015-8362.	22/01/2016	10.0	CVE-2016-1984
hospira -- lifecare_pca_infusion_system	Stack-based buffer overflow in Hospira Communication Engine (CE) before 1.2 in LifeCare PCA Infusion System 5.07, Plum A+ Infusion System 13.40, and Plum A+3 Infusion System 13.40 allows remote attackers to cause a denial of service or possibly have unspecified other impact via traffic on TCP port 5000.	22/01/2016	10.0	CVE-2015-7909

Semana 18/01/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cgit_project -- cgit	Integer overflow in the authenticate_post function in CGit before 0.12 allows remote attackers to have unspecified impact via a large value in the Content-Length HTTP header, which triggers a buffer overflow.	20/01/2016	7.5	CVE-2016-1901
sap -- hana	Buffer overflow in the XS engine (hdbxsengine) in SAP HANA allows remote attackers to cause a denial of service or execute arbitrary code via a crafted HTTP request, related to JSON, aka SAP Security Note 2241978.	20/01/2016	7.5	CVE-2016-1928
sap -- hana	The XS engine in SAP HANA allows remote attackers to spoof log entries in trace files and consequently cause a denial of service (disk consumption and process crash) via a crafted HTTP request, related to an unspecified debug function, aka SAP Security Note 2241978.	20/01/2016	8.5	CVE-2016-1929
php -- php	Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension.	19/01/2016	7.5	CVE-2015-5590
php -- php	The php_str_replace_in_subject function in ext/standard/string.c in PHP 7.x before 7.0.0 allows remote attackers to execute arbitrary code via a crafted value in the third argument to the str_ireplace function.	19/01/2016	7.5	CVE-2015-6527
php -- php	Multiple use-after-free vulnerabilities in SPL in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allow remote attackers to execute arbitrary code via vectors involving (1) ArrayObject, (2) SplObjectStorage, and (3) SplDoublyLinkedList, which are mishandled during unserialization.	19/01/2016	7.5	CVE-2015-6831
php -- php	Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array field.	19/01/2016	7.5	CVE-2015-6832
php -- php	The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function.	19/01/2016	7.5	CVE-2015-6836
php -- php	Use-after-free vulnerability in the Collator::sortWithSortKeys function in ext/intl/collator/collator_sort.c in PHP 7.x before 7.0.1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging the relationships between a key buffer and a destroyed array.	19/01/2016	7.5	CVE-2015-8616
php -- php	Format string vulnerability in the zend_throw_or_error function in Zend/zend_execute_API.c in PHP 7.x before 7.0.1 allows remote attackers to execute arbitrary code via format string specifiers in a string that is misused as a class name, leading to incorrect error handling.	19/01/2016	10.0	CVE-2015-8617
php -- php	Multiple integer overflows in ext/standard/exec.c in PHP 7.x before 7.0.2 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a long string to the (1) php_escape_shell_cmd or (2) php_escape_shell_arg function, leading to a heap-based buffer overflow.	19/01/2016	7.5	CVE-2016-1904
ibm -- tealeaf_customer_experience	Directory traversal vulnerability in the replay server in IBM Tealeaf Customer Experience before 8.7.1.8818, 8.8 before 8.8.0.9026, 9.0.0, 9.0.0A, 9.0.1 before 9.0.1.1083, 9.0.1A before 9.0.1.5073, 9.0.2 before 9.0.2.1095, and 9.0.2A before 9.0.2.5144 allows remote attackers to read arbitrary files via unspecified vectors.	18/01/2016	7.8	CVE-2015-4988
hp -- arcsight_logger	HPE ArcSight Logger before 6.1P1 allows remote attackers to execute arbitrary code via unspecified input to the (1) Intellicus or (2) client-certificate upload component.	16/01/2016	7.5	CVE-2015-6863
seeds -- acmailer	Seeds acmailer before 3.8.21 and 3.9.x before 3.9.15 Beta allows remote authenticated users to execute arbitrary OS commands via unspecified vectors.	16/01/2016	9.0	CVE-2016-1142
fortinet -- fortios	FortiOS 4.x before 4.3.17 and 5.0.x before 5.0.8 has a hardcoded passphrase for the Fortimanager_Access account, which allows remote attackers to obtain administrative access via an SSH session.	15/01/2016	10.0	CVE-2016-1909

Semana 11/01/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946.	14/01/2016	10.0	CVE-2016-0933
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted JPEG 2000 data, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946.	14/01/2016	9.3	CVE-2016-0936
adobe -- acrobat	Use-after-free vulnerability in the OCG object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0940, and CVE-2016-0941.	14/01/2016	9.3	CVE-2016-0937
adobe -- acrobat	The AcroForm plugin in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946.	14/01/2016	9.3	CVE-2016-0938
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, and CVE-2016-0941.	14/01/2016	10.0	CVE-2016-0940
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946.	14/01/2016	10.0	CVE-2016-0942
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0945, and CVE-2016-0946.	14/01/2016	10.0	CVE-2016-0944
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, and CVE-2016-0946.	14/01/2016	10.0	CVE-2016-0945
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, and CVE-2016-0945.	14/01/2016	10.0	CVE-2016-0946
adobe -- acrobat	Untrusted search path vulnerability in Adobe Download Manager, as used in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X, allows local users to gain privileges via a crafted resource in an unspecified directory.	14/01/2016	7.2	CVE-2016-0947
microsoft -- jscript	The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	13/01/2016	9.3	CVE-2016-0002
microsoft -- edge	Microsoft Edge allows remote attackers to execute arbitrary code via unspecified vectors, aka "Microsoft Edge Memory Corruption Vulnerability."	13/01/2016	9.3	CVE-2016-0003
microsoft -- windows_10	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 10 Gold and 1511 allow remote attackers to execute arbitrary code via unspecified vectors, aka "Win32k Remote Code Execution Vulnerability."	13/01/2016	9.3	CVE-2016-0009
microsoft -- excel_for_mac	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, Office 2016, Excel for Mac 2011, PowerPoint for Mac 2011, Word for Mac 2011, Excel 2016 for Mac, PowerPoint 2016 for Mac, Word 2016 for Mac, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	13/01/2016	9.3	CVE-2016-0010
microsoft -- windows_10	DirectShow in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka "DirectShow Heap Corruption Remote Code Execution Vulnerability."	13/01/2016	9.3	CVE-2016-0015
microsoft -- windows_10	The Remote Desktop Protocol (RDP) service implementation in Microsoft Windows 10 Gold and 1511 allows remote attackers to bypass intended access restrictions and establish sessions for blank-password accounts via a modified RDP client, aka "Windows Remote Desktop Protocol Security Bypass Vulnerability."	13/01/2016	9.3	CVE-2016-0019
microsoft -- windows_7	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "MAPI DLL Loading Elevation of Privilege Vulnerability."	13/01/2016	7.2	CVE-2016-0020
microsoft -- edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via unspecified vectors, aka "Scripting Engine Memory Corruption Vulnerability."	13/01/2016	9.3	CVE-2016-0024
microsoft -- silverlight	Microsoft Silverlight 5 before 5.1.41212.0 mishandles negative offsets during decoding, which allows remote attackers to execute arbitrary code or cause a denial of service (object-header corruption) via a crafted web site, aka "Silverlight Runtime Remote Code Execution Vulnerability."	13/01/2016	9.3	CVE-2016-0034
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 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."	13/01/2016	9.3	CVE-2016-0035

Histórico de vulnerabilidades de Enero del 2016

	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip_access_policy_manager	F5 BIG-IP APM 11.4.1 before 11.4.1 HF9, 11.5.x before 11.5.3, and 11.6.0 before 11.6.0 HF4 allow remote attackers to cause a denial of service or execute arbitrary code via unspecified vectors related to processing a Citrix Remote Desktop connection through a virtual server configured with a remote desktop profile, aka an "Out-of-bounds memory vulnerability."	12/01/2016	10.0	CVE-2015-8098
f5 -- big-ip_access_policy_manager	BIG-IP LTM, AAM, AFM, Analytics, APM, ASM, DNS, Link Controller, and PEM 12.0.0 before HF1 on the 2000, 4000, 5000, 7000, and 10000 platforms do not properly sync passwords with the Always-On Management (AOM) subsystem, which might allow remote attackers to obtain login access to AOM via an (1) expired or (2) default password.	12/01/2016	10.0	CVE-2015-8611
huawei -- mate_7_firmware	Heap-based buffer overflow in the HIFI driver in Huawei Mate 7 phones with software MT7-UL00 before MT7-UL00C17B354, MT7-TL10 before MT7-TL10C00B354, MT7-TL00 before MT7-TL00C01B354, and MT7-CL00 before MT7-CL00C92B354 and P8 phones with software GRA-TL00 before GRA-TL00C01B220SP01, GRA-CL00 before GRA-CL00C92B220, GRA-CL10 before GRA-CL10C92B220, GRA-UL00 before GRA-UL00C00B220, and GRA-UL10 before GRA-UL10C00B220 allows attackers to cause a denial of service (reboot) or execute arbitrary code via a crafted application.	12/01/2016	9.3	CVE-2015-8088
joomla -- joomla\!	SQL injection vulnerability in Joomla! 3.x before 3.4.7 allows attackers to execute arbitrary SQL commands via unspecified vectors.	12/01/2016	7.5	CVE-2015-8769
qemu -- qemu	The VNC websocket frame decoder in QEMU allows remote attackers to cause a denial of service (memory and CPU consumption) via a large (1) websocket payload or (2) HTTP headers section.	12/01/2016	7.8	CVE-2015-1779
apple -- mac_os_x	Directory Utility in Apple OS X before 10.11.1 mishandles authentication for new sessions, which allows local users to gain privileges via unspecified vectors.	11/01/2016	7.2	CVE-2015-6980
huawei -- espace_8950	Memory leak in Huawei eSpace 8950 IP phones with software before V200R003C00SPC300 allows remote attackers to cause a denial of service (memory consumption and restart) via a large number of crafted ARP packets.	11/01/2016	7.8	CVE-2015-8230
huawei -- espace_7910	Huawei eSpace 7910 and 7950 IP phones with software before V200R002C00SPC800 allow remote attackers with established sessions to cause a denial of service (device restart) via unspecified packets.	11/01/2016	7.8	CVE-2015-8231
zarafa -- zarafa_collaboration_platform	zarafa-autorespond in Zarafa Collaboration Platform (ZCP) before 7.2.1 allows local users to gain privileges via a symlink attack on /tmp/zarafa-vacation-*.	11/01/2016	7.2	CVE-2015-6566
apache -- activemq	Apache ActiveMQ 5.x before 5.13.0 does not restrict the classes that can be serialized in the broker, which allows remote attackers to execute arbitrary code via a crafted serialized Java Message Service (JMS) ObjectMessage object.	08/01/2016	7.5	CVE-2015-5254
apache -- subversion	Integer overflow in the read_string function in libsvn_ra_svn/marshal.c in Apache Subversion 1.9.x before 1.9.3 allows remote attackers to execute arbitrary code via an svn:// protocol string, which triggers a heap-based buffer overflow and an out-of-bounds read.	08/01/2016	9.0	CVE-2015-5259
avm -- fritz!_os	AVM FRITZ!OS before 6.30 extracts the contents of firmware updates before verifying their cryptographic signature, which allows remote attackers to create symlinks or overwrite critical files, and consequently execute arbitrary code, via a crafted firmware image.	08/01/2016	9.3	CVE-2014-8886
blueman_project -- blueman	The EnableNetwork method in the Network class in plugins/mechanism/Network.py in Blueman before 2.0.3 allows local users to gain privileges via the dhcp_handler argument.	08/01/2016	7.2	CVE-2015-8612
dell -- pre-boot_authentication_driver	Dell Pre-Boot Authentication Driver (PBADRV.sys) 1.0.1.5 allows local users to write to arbitrary physical memory locations and gain privileges via a 0x0022201c IOCTL call.	08/01/2016	7.2	CVE-2015-6856
fortinet -- forticlient	Fortinet FortiClient Linux SSLVPN before build 2313, when installed on Linux in a home directory that is world readable and executable, allows local users to gain privileges via the helper/subroc setuid program.	08/01/2016	7.2	CVE-2015-7362
huawei -- ale_firmware	The Joint Photographic Experts Group Processing Unit (JPU) driver in Huawei ALE smartphones with software before ALE-UL00C00B220 and ALE-TL00C01B220 and GEM-703L smartphones with software before V100R001C233B111 allows remote attackers to cause a denial of service (crash) via a crafted application with the system or camera permission, a different vulnerability than CVE-2015-8226.	08/01/2016	7.1	CVE-2015-8225
huawei -- ale_firmware	The Joint Photographic Experts Group Processing Unit (JPU) driver in Huawei ALE smartphones with software before ALE-UL00C00B220 and ALE-TL00C01B220 and GEM-703L smartphones with software before V100R001C233B111 allows remote attackers to cause a denial of service (crash) via a crafted application with the system or camera permission, a different vulnerability than CVE-2015-8225.	08/01/2016	7.1	CVE-2015-8226
juniper -- screenos	Juniper ScreenOS before 6.3.0r21, when ssh-pka is configured and enabled, allows remote attackers to cause a denial of service (system crash) or execute arbitrary code via crafted SSH negotiation.	08/01/2016	9.3	CVE-2015-7754
libtiff_project -- libtiff	The _TIFFVGetField function in tif_dir.c in libtiff 4.0.6 allows attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via crafted field data in an extension tag in a TIFF image.	08/01/2016	7.5	CVE-2015-7554
libtiff_project -- libtiff	Heap-based buffer overflow in the PackBitsPreEncode function in tif_packbits.c in bmp2tiff in libtiff 4.0.6 and earlier allows remote attackers to execute arbitrary code or cause a denial of service via a large width field in a BMP image.	08/01/2016	7.5	CVE-2015-8668
mcafee -- epolicy_orchestrator	Intel McAfee ePolicy Orchestrator (ePO) 4.6.9 and earlier, 5.0.x, 5.1.x before 5.1.3 Hotfix 1106041, and 5.3.x before 5.3.1 Hotfix 1106041 allow remote attackers to execute arbitrary code via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	08/01/2016	7.5	CVE-2015-8765
owncloud -- owncloud	ownCloud Server before 8.0.10, 8.1.x before 8.1.5, and 8.2.x before 8.2.2 allow remote authenticated users to obtain sensitive information from a directory listing and possibly cause a denial of service (CPU consumption) via the force parameter to index.php/apps/files/ajax/scan.php.	08/01/2016	7.5	CVE-2016-1499
pygments -- pygments	The FontManager._get_nix_font_path function in formatters/img.py in Pygments 1.2.2 through 2.0.2 allows remote attackers to execute arbitrary commands via shell metacharacters in a font name.	08/01/2016	9.3	CVE-2015-8557
sap -- afaria	SAP Afaria 7.0.6001.5 allows remote attackers to bypass authorization checks and wipe or lock mobile devices via a crafted request, related to "Insecure signature," aka SAP Security Note 2134905.	08/01/2016	9.4	CVE-2015-8753

Semana 04/01/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- ucmdb_browser	HPE UCMDB Browser before 4.02 allows remote attackers to obtain sensitive information or bypass intended access restrictions via unspecified vectors.	07/01/2016	7.2	CVE-2015-6862
ipswitch -- whatsup_gold	The DroneDeleteOldMeasurements implementation in Ipswitch WhatsUp Gold before 16.4 does not properly validate serialized XML objects, which allows remote attackers to conduct SQL injection attacks via a crafted SOAP request.	07/01/2016	7.5	CVE-2015-8261
google -- android	mediaserver in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bugs 25070493 and 24686670.	06/01/2016	10.0	CVE-2015-6636
google -- android	The MediaTek misc-sd driver in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application, aka internal bug 25307013.	06/01/2016	9.3	CVE-2015-6637
google -- android	The Imagination Technologies driver in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application, aka internal bug 24673908.	06/01/2016	9.3	CVE-2015-6638
google -- android	The Widevine QSEE TrustZone application in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application that leverages QSEECOM access, aka internal bug 24446875.	06/01/2016	9.3	CVE-2015-6639
google -- android	The prctl_set_vma_anon_name function in kernel/sys.c in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 does not ensure that only one vma is accessed in a certain update action, which allows attackers to gain privileges or cause a denial of service (vma list corruption) via a crafted application, aka internal bug 20017123.	06/01/2016	9.3	CVE-2015-6640
google -- android	The kernel in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, via unknown vectors, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 24157888.	06/01/2016	7.8	CVE-2015-6642
google -- android	Setup Wizard in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows physically proximate attackers to modify settings or bypass a reset protection mechanism via unspecified vectors, aka internal bug 25290269.	06/01/2016	7.2	CVE-2015-6643
google -- android	SyncManager in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to cause a denial of service (continuous rebooting) via a crafted application, aka internal bug 23591205.	06/01/2016	7.1	CVE-2015-6645
google -- android	The System V IPC implementation in the kernel in Android before 6.0 2016-01-01 allows attackers to cause a denial of service (global kernel resource consumption) by leveraging improper interaction between IPC resource allocation and the memory manager, aka internal bug 22300191, a different vulnerability than CVE-2015-7613.	06/01/2016	7.8	CVE-2015-6646
google -- android	The Widevine QSEE TrustZone application in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application that leverages QSEECOM access, aka internal bug 24441554.	06/01/2016	9.3	CVE-2015-6647
hp -- j8692a	HPE Network Switches with software 15.16.x and 15.17.x allow local users to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-6859.	05/01/2016	7.2	CVE-2015-6860
ibm -- tivoli_monitoring	The portal in IBM Tivoli Monitoring (ITM) 6.2.2 through FP9, 6.2.3 through FP5, and 6.3.0 before FP7 allows remote authenticated users to execute arbitrary commands by leveraging Take Action view authority and providing crafted input.	03/01/2016	8.5	CVE-2015-5003
ibm -- connections	IBM Connections 3.x before 3.0.1.1 CR3, 4.0 before CR4, 4.5 before CR5, and 5.0 before CR3 does not properly detect recursion during XML entity expansion, which allows remote attackers to cause a denial of service (CPU consumption and application crash) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.	03/01/2016	7.8	CVE-2015-5038
ibm -- i_access	Buffer overflow in IBM i Access 7.1 on Windows allows local users to gain privileges via unspecified vectors.	02/01/2016	7.2	CVE-2015-2023
ibm -- security_access_manager_9.0_firmware	IBM Security Access Manager for Web 7.0.0 before FP19 and 8.0 before 8.0.1.3 IF3, and Security Access Manager 9.0 before 9.0.0.0 IF1, allows remote authenticated users to execute arbitrary OS commands by leveraging Local Management Interface (LMI) access.	02/01/2016	8.5	CVE-2015-5018
ibm -- spectrum_protect_for_virtual_environments	The Data Protection extension in the VMware GUI in IBM Tivoli Storage Manager for Virtual Environments: Data Protection for VMware (aka Spectrum Protect for Virtual Environments) 7.1 before 7.1.3.0 and Tivoli Storage FlashCopy Manager for VMware (aka Spectrum Protect Snapshot) 4.1 before 4.1.3.0 allows remote attackers to execute arbitrary OS commands via unspecified vectors.	02/01/2016	10.0	CVE-2015-7426
ibm -- tivoli_common_reporting	IBM Tivoli Common Reporting (TCR) 2.1 before IF14, 2.1.1 before IF22, 2.1.1.2 before IF9, 3.1.0.0 through 3.1.2 as used in Cognos Business Intelligence before 10.2 IF16, and 3.1.2.1 as used in Cognos Business Intelligence before 10.2.1.1 IF12 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the InvokerTransformer class in the Apache Commons Collections library.	02/01/2016	10.0	CVE-2015-7450
pcre -- perl_compatible_regular_expression_library	The pcre_compile2 function in pcre_compile.c in PCRE 8.38 mishandles the /((?:F?+(?:^(?(R)a+\"){99}-))(?J)(?'R'(?'R'<((?'RR'(?'R'\){97)?J)?J)(?'R'(?'R'\){99|(:(?|(?'R')(\k'R')|((?'R')))H'R'R)(H'R))))))/ pattern and related patterns with named subgroups, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	02/01/2016	7.5	CVE-2016-1283