

Histórico de vulnerabilidades de Junio del 2016

Semana 27/06/2016					
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info	
apple - mDNSResponder	The handle_request function in mDNSResponder before 625.41.2 allows remote attackers to execute arbitrary code or cause a denial of service (NULL pointer dereference) via unspecified vectors.	25/06/2016	7.5	CVE-2016-7088	
corega - ig-wlbaragm_firmware	Corega CG-WLBARAGM devices allow remote attackers to cause a denial of service (reboot) via unspecified vectors.	25/06/2016	7.8	CVE-2016-6823	
fs - big-ip_access_policy_manager	FS BIG-IP before 12.0.0.H3 allows remote authenticated users to modify the account configuration of users with the Resource Administration role and gain privilege via a crafted external Extended Application Verification (EAV) monitor script.	30/06/2016	9.0	CVE-2016-5020	
huawei - mate_8_firmware	Buffer overflow in Huawei Mate8 NKT-AL before NKT-ALD000B182, NKT-CL before NKT-CLD000S28182, NKT-DL before NKT-DL000L7B182, and NKT-TL before NKT-TL000T1B182 allows attackers to cause a denial of service (system crash) via a crafted app.	30/06/2016	7.1	CVE-2016-5233	
huawei - ar3200_firmware	Memory leak in Huawei AR3200 before V200R007C00SPC900 allows remote attackers to cause a denial of service (memory consumption) via a large number of crafted MultiProtocol Label Switching (MPLS) packets.	30/06/2016	7.8	CVE-2016-5268	
huawei - huawei_firmware	Memory leak in Huawei IPS Module, NGFW Module, NIP6600, NIP6600, and Secospace USG6300, USG6600, USG9500, and AntiDDoS8000 V500R001C00 before V500R001C00SPC100, when in hot standby networking where two devices are not directly connected, allows remote attackers to cause a denial of service (memory consumption and reboot) via a crafted packet.	24/06/2016	7.1	CVE-2016-5435	
huawei - ocean_stor_firmware	ovsactor 5300 V1, 5500 V1, 5600 V1, 5800 V1, 6800 V1, 18800 V1, and 18500 V3 before V1000R01C10 sends the plaintext session token in the HTTP header, which allows remote attackers to conduct replay attacks and obtain sensitive information by sniffing the network.	24/06/2016	7.5	CVE-2016-5722	
huawei - fusioninsight_hd	Huawei FusionInsight HD before V100R002C05PC200 allows local users to gain root privileges via unspecified vectors.	24/06/2016	7.2	CVE-2016-5724	
ibm - marketing_platform	SQL injection vulnerability in IBM Marketing Platform 8.5.x, 8.6.x, and 9.x before 9.1.2.2 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	27/06/2016	7.5	CVE-2016-0224	
ibm - general_parallel_file_system_storage_service	IBM Spectrum Scale 4.1 before 4.1.1.5 and 4.2 before 4.2.0.2 and General Parallel File System 3.5 before 3.5.0.30 allow local users to gain privileges or cause a denial of service via a crafted mmappphlycopy command.	28/06/2016	7.8	CVE-2016-0263	
ibm - messagesight	JMS Client in IBM MessageSight 1.1.x through 1.1.0.1, 1.2.x through 1.2.0.3, and 2.0.x through 2.0.0.0 allows remote authenticated users to obtain administrator privileges for executing arbitrary commands via unspecified vectors.	30/06/2016	9.0	CVE-2016-0275	
lenovo - solution_center	Lenovo Solution Center (LSC) before 3.3.003 allows local users to execute arbitrary code with LocalSystem privileges via vectors involving the LSC.Services.SystemService.StartProxy command with a named pipe created in advance and crafted .NET assembly.	30/06/2016	7.2	CVE-2016-5249	
linux - linux_kernel	Integer overflow in the snd_compr_allocate_buffer function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.16-r6-next-20120917 allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call.	29/06/2016	7.2	CVE-2012-6703	
linux - linux_kernel	The snd_compr_check_input function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.17 does not properly check for an integer overflow, which allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call.	27/06/2016	7.2	CVE-2014-9904	
linux - linux_kernel	Integer overflow in the hwm1_decoder in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.	27/06/2016	7.2	CVE-2016-0738	
linux - linux_kernel	The cryptfs_privileged_open function in fs/cryptfs/hwthread.c in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (stack memory consumption) via vectors involving crafted mount calls for /proc/pidnames, leading to recursive caefault handling.	27/06/2016	7.2	CVE-2016-1583	
linux - linux_kernel	arch/86/kvm/kvm.c in the Linux kernel through 4.6.3 mishandles the APIC on/off state, which allows guest OS users to obtain direct APIC MSR access on the host OS, and consequently cause a denial of service (host OS crash) or possibly execute arbitrary code on the host OS via xAPIC mode.	27/06/2016	7.2	CVE-2016-4440	
linux - linux_kernel	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transitional state, which allows local users to cause a denial of service (invalid process state or TM bad thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an emc system call.	27/06/2016	7.2	CVE-2016-5828	
linux - linux_kernel	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGE64 or (2) HIDIOCGUSAGE32 ioctl call.	27/06/2016	7.2	CVE-2016-5829	
opera - opera_mail	Unspecified vulnerability in Opera Mail before 2016-03-16 on Windows allows user-assisted remote attackers to execute arbitrary code via a crafted e-mail message.	29/06/2016	9.3	CVE-2016-5101	
siemens - simatic_37_300_with_profinet_support_firmware	Siemens SIMATIC S7 300 Profinet-enabled CPU devices with firmware before 3.2.12 and SIMATIC S7 300 Profinet disabled CPU devices with firmware before 3.8.12 allow remote attackers to cause a denial of service (defect-mode transition) via crafted (1) ISO-TSAP or (2) ProfBus packets.	27/06/2016	7.8	CVE-2016-8949	
symphony-cms - symphony_cms	Session fixation vulnerability in Symphony CMS 2.6.7, when session use_only_cookies is disabled, allows remote attackers to hijack web sessions via the PHPSESSID parameter.	30/06/2016	7.8	CVE-2016-4309	
trend-micro - deep_discovery_inspector	Hosts_upload.cgi in Trend Micro Deep Discovery Inspector (DDI) 3.7, 3.8 SP1 (3.8.1), and 3.8 SP3 (3.8.2) allows remote administrators to execute arbitrary code via a crafted string.	30/06/2016	9.0	CVE-2016-5840	
unitronics - vollogc_optic_ide	Stack-based buffer overflow in Unitronics VolLogc OPTIC IDE before 9.8.30 allows remote attackers to execute arbitrary code via a crafted filename field in a ZIP archive in a zip file.	24/06/2016	7.5	CVE-2016-4519	

Semana 20/06/2016					
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info	
apple - mac_os_x	The NVIDIA Graphics Drivers subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1846.	19/06/2016	9.3	CVE-2016-1861	
dx_library_project - dx_library	The printf function in Takumi Yamada DX Library for Borland C++ 3.13F through 3.16B, DX Library for Gnu C++ 3.13F through 3.16B, and DX Library for Visual C++ 3.13F through 3.16B allows remote attackers to execute arbitrary code via a crafted string.	18/06/2016	7.5	CVE-2016-4819	
emc - data_domain	EMC Data Domain OS 5.4 through 5.7 before 5.7.2.0 has a default no_root_squash option for NFS exports, which makes it easier for remote attackers to obtain file system access by leveraging client root privileges.	19/06/2016	7.2	CVE-2016-0911	
emc - data_domain	EMC Data Domain OS 5.4 through 5.7 before 5.7.2.0 allows remote authenticated users to bypass intended password-change restrictions by leveraging access to (1) a different account with the same role as a target account or (2) an account's session at an unattended workstation.	19/06/2016	9.0	CVE-2016-0912	
fortality - fortality	Fortality (previously Tribex Pro) 12.6 through 14.1 before 2016-06-01 has a hardcoded password for the FTP account, which allows remote attackers to obtain access via a FTP FTP or FTP SMT connection.	19/06/2016	10.0	CVE-2016-2362	
fortality - fortality	Fortality (previously Tribex Pro) 12.6 through 14.1 before 2016-06-01 uses weak permissions for the /var/www/ftp/surion script, which allows local users to obtain root access for unspecified command execution by leveraging access to the nobody account.	19/06/2016	7.2	CVE-2016-2163	
netcommons - netcommons	NetCommons 2.2.1 and earlier allows remote authenticated secretanar (aka CLERK) users to gain privileges by creating a SYSTEM_ADMIN account.	18/06/2016	9.0	CVE-2016-4813	
openssl - openssl	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by generating unexpected malloc behavior, related to ssl_openssl_ssl_sess.c and 11_lib.c.	19/06/2016	7.5	CVE-2016-2177	
solarwinds - virtualization_manager	The RMI service in SolarWinds Virtualization Manager 6.3.1 and earlier allows remote attackers to execute arbitrary commands via crafted external packets, related to the Apache Commons Collections (CC) library.	17/06/2016	10.0	CVE-2016-3942	
solarwinds - virtualization_manager	SolarWinds Virtualization Manager 6.3.1 and earlier allow local users to gain privileges by leveraging a misconfiguration of sudo, as demonstrated by "sudo cat /etc/passwd".	17/06/2016	7.2	CVE-2016-3848	

Semana 13/06/2016					
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info	
adobe - air_desktop_runtime	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4156, CVE-2016-4161, CVE-2016-4162, and CVE-2016-4164.	16/06/2016	7.5	CVE-2016-4120	
adobe - air_desktop_runtime	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1097, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, and CVE-2016-4110.	16/06/2016	7.5	CVE-2016-4121	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4122	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4123	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4124	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4125	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4126	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4127	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	10.0	CVE-2016-4128	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	10.0	CVE-2016-4129	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4130	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4131	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4132	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4133	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4134	
adobe - flash_player	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	16/06/2016	9.3	CVE-2016-4135	



Histórico de vulnerabilidades de Junio del 2016

Primary Vendor / Product	Description	Published	CVSS Score	Source & Patch Info
google - android	mp3decSoftMP3.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 2016-06-01 does not validate the relationship between allocated memory and the frame size, which allows attackers to gain privileges via a crafted application, aka internal bug 27793371	12/06/2016	9.3	<a href="#">CVE-2016-2486</a>
google - android	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 2016-06-01 allows attackers to gain privileges via a crafted application, aka internal bug 27793371	12/06/2016	9.3	<a href="#">CVE-2016-2487</a>
google - android	The Qualcomm camera driver in Android before 2016-06-01 on Nexus 5, 5X, 6, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 27600832	12/06/2016	9.3	<a href="#">CVE-2016-2488</a>
google - android	The Qualcomm video driver in Android before 2016-06-01 on Nexus 5, 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 27407079	12/06/2016	9.3	<a href="#">CVE-2016-2489</a>
google - android	The NVIDIA camera driver in Android before 2016-06-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27531373	12/06/2016	9.3	<a href="#">CVE-2016-2490</a>
google - android	The NVIDIA camera driver in Android before 2016-06-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27556408	12/06/2016	9.3	<a href="#">CVE-2016-2491</a>
google - android	The MediaTek power-management driver in Android before 2016-06-01 on Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 28085410	12/06/2016	9.3	<a href="#">CVE-2016-2492</a>
google - android	The Broadcom Wi-Fi driver in Android before 2016-06-01 on Nexus 5, Nexus 6, Nexus 6P, Nexus 7 (2013), Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 28074322	12/06/2016	9.3	<a href="#">CVE-2016-2493</a>
google - android	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 2016-06-01 allows attackers to gain privileges via a crafted application, aka internal bug 28055498	12/06/2016	9.3	<a href="#">CVE-2016-2494</a>
google - android	SampleTable.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 2016-06-01 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28076789	12/06/2016	7.1	<a href="#">CVE-2016-2495</a>
google - android	The Framework UI permission-dialog implementation in Android 6.x before 2016-06-01 allows attackers to conduct tapping attacks and access arbitrary private-storage files by creating a partially overlapping window, aka internal bug 26677706	12/06/2016	10.0	<a href="#">CVE-2016-2496</a>
graphicsmagick - graphicsmagick	The OpenJpeg function in lib.c in GraphicsMagick before 1.3.24 and ImageMagick allows remote attackers to execute arbitrary code via a   (pipe) character at the start of a filename.	10/06/2016	10.0	<a href="#">CVE-2016-5118</a>
huawei - hiLink_app	The Huawei HiLink App application before 3.19.2 for Android does not validate SSL certificates, which allows local users to have unspecified impact via unspecified vectors, aka HWPSIRT-2016-05008	13/06/2016	7.5	<a href="#">CVE-2016-4605</a>
huawei - rs6500_firmware	Buffer overflow in Huawei VP9660, VP9650, and VP9630 multipoint control unit devices with software before V500R002C00SPC200 and RS6500 videoconference devices with software before V500R002C00SPC100, when an unspecified service is enabled, allows remote attackers to execute arbitrary code via a crafted packet, aka HWPSIRT-2016-05054	13/06/2016	9.3	<a href="#">CVE-2016-5334</a>
huawei - honor_wd851_firmware	Stack-based buffer overflow in Huawei Honor WS851 routers with software 1.1.2.1.1 and earlier allows remote attackers to execute arbitrary code via a crafted packet, aka HWPSIRT-2016-05051	14/06/2016	10.0	<a href="#">CVE-2016-5305</a>
libexpat - expat	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0876.	16/06/2016	7.8	<a href="#">CVE-2016-5300</a>
linux - linux_kernel	Integer signedness error in the MSM V4L2 video driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges or cause a denial of service (array overflow and memory corruption) via a crafted application that triggers an mmio_tpm_aml_create_stream call.	12/06/2016	9.3	<a href="#">CVE-2016-2963</a>
linux - linux_kernel	Integer signedness error in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges or cause a denial of service (memory corruption) via a crafted application that makes an ioctl call.	12/06/2016	9.3	<a href="#">CVE-2016-2966</a>
microsoft - office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office 2016, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-0025</a>
microsoft - internet_explorer	Microsoft Internet Explorer 9 through 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," a different vulnerability than CVE-2016-0200 and CVE-2016-0211	15/06/2016	9.3	<a href="#">CVE-2016-0199</a>
microsoft - internet_explorer	Microsoft Internet Explorer 9 through 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," a different vulnerability than CVE-2016-0199 and CVE-2016-0211	15/06/2016	9.3	<a href="#">CVE-2016-0200</a>
microsoft - edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0214	15/06/2016	9.3	<a href="#">CVE-2016-0199</a>
microsoft - chakra_javascript	The Microsoft (1) Chakra JavaScript, (2) JScript, and (3) VBScript engines, as used in Microsoft Internet Explorer 10 and 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 "Scripting Engine Memory Corruption Vulnerability."	15/06/2016	7.6	<a href="#">CVE-2016-3200</a>
microsoft - edge	Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to execute arbitrary code via a crafted PDF document, aka "Windows PDF Remote Code Execution Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-3103</a>
microsoft - jscript	The Microsoft (1) JScript 5.8 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3206 and CVE-2016-3207.	15/06/2016	7.6	<a href="#">CVE-2016-3205</a>
microsoft - jscript	The Microsoft (1) JScript 5.8 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3205 and CVE-2016-3207.	15/06/2016	9.3	<a href="#">CVE-2016-3206</a>
microsoft - jscript	The Microsoft (1) JScript 5.8 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3205 and CVE-2016-3207.	15/06/2016	7.6	<a href="#">CVE-2016-3207</a>
microsoft - internet_explorer	The Microsoft (1) JScript and (2) VBScript engines, as used in Internet Explorer 11, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-3210</a>
microsoft - internet_explorer	Microsoft Internet Explorer 9 through 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," a different vulnerability than CVE-2016-0199 and CVE-2016-0200	15/06/2016	9.3	<a href="#">CVE-2016-3211</a>
microsoft - internet_explorer	The Web Proxy Auto Discovery (WPAD) protocol implementation 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, and Internet Explorer 9 through 11 has an improper fallback mechanism, which allows remote attackers to gain privileges via NetBIOS name responses, aka "WPAD Elevation of Privilege Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-3213</a>
microsoft - edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0214	15/06/2016	9.3	<a href="#">CVE-2016-3214</a>
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."	15/06/2016	9.3	<a href="#">CVE-2016-3222</a>
microsoft - windows_10	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 mishandle LDAP authentication, which allows man-in-the-middle attackers to gain privileges by modifying group-policy update data within a domain-controller data stream, aka "Group Policy Elevation of Privilege Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-3223</a>
microsoft - windows_server_2012	Use-after-free vulnerability in the DNS Server component in Microsoft Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted requests, aka "Windows DNS Server Use After Free Vulnerability."	15/06/2016	10.0	<a href="#">CVE-2016-3227</a>
microsoft - windows_server_2008	Microsoft Windows Server 2008 SP2 and R2 SP1 and Windows Server 2012 Gold and R2 allow remote authenticated users to execute arbitrary code via a crafted NetLogon request, aka "Windows Netlogon Memory Corruption Remote Code Execution Vulnerability."	15/06/2016	9.0	<a href="#">CVE-2016-3228</a>
microsoft - windows_diagnostics_hub	The Standard Collector service in Windows Diagnostics Hub mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Microsoft Office Memory Corruption Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-3231</a>
microsoft - excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-3232</a>
microsoft - visio	Microsoft Visio 2007 SP3, Visio 2010 SP1, Visio 2013 SP1, Visio 2016, Visio Viewer 2007 SP3, and Visio Viewer 2010 mishandle library loading, which allows local users to gain privileges via a crafted application, aka "Microsoft Office OLE DLL Side Loading Vulnerability."	15/06/2016	9.3	<a href="#">CVE-2016-3235</a>
microsoft - windows_10	The Web Proxy Auto Discovery (WPAD) protocol implementation 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 mishandles proxy discovery, which allows remote attackers to redirect network traffic via unspecified vectors, aka "Windows WPAD Proxy Discovery Elevation of Privilege Vulnerability."	15/06/2016	10.0	<a href="#">CVE-2016-3236</a>
mozilla - firefox	The maintenance service in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 on Windows does not prevent MAA extracted file modification during update execution, which might allow local users to gain privileges via a Trojan horse file.	13/06/2016	7.2	<a href="#">CVE-2016-2826</a>
mozilla - firefox	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.	13/06/2016	9.3	<a href="#">CVE-2016-2834</a>
puppetlabs - puppet	Puppet Server before 2.3.2 and Ruby puppetmaster in Puppet 4.x before 4.4.2 and in Puppet Agent before 1.4.2 might allow remote attackers to bypass intended auth.conf access restrictions by leveraging incorrect URL decoding.	10/06/2016	7.5	<a href="#">CVE-2016-2785</a>
puppetlabs - puppet_agent	The pre-agent component in Puppet Enterprise 2015.3.x before 2015.3.3 and Puppet Agent 1.x before 1.3.6 does not properly validate server certificates, which might allow remote attackers to spoof brokers and execute arbitrary commands via a crafted certificate.	10/06/2016	7.5	<a href="#">CVE-2016-2786</a>
solarwinds - virtualization_manager	The RM service in SolarWinds Virtualization Manager 6.3.1 and earlier allows remote attackers to execute arbitrary commands via a crafted serialized 'isaObject' related to the Apache Commons Collections (ACC) library.	17/06/2016	10.0	<a href="#">CVE-2016-3642</a>
solarwinds - virtualization_manager	SolarWinds Virtualization Manager 6.3.1 and earlier allow local users to gain privileges by leveraging a misconfiguration of sudo, as demonstrated by "sudo cat /etc/passwd"	17/06/2016	7.2	<a href="#">CVE-2016-3643</a>

Histórico de vulnerabilidades de Junio del 2016

Semana 06/06/2016				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
Novell-opensuse	Stack-based buffer overflow in the <code>dnsmip_call</code> function in <code>unrpcdnt_udp.c</code> in the GNU C Library (aka glibc or libc) allows remote servers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.	10/06/2016	7.5	<a href="#">CVE-2016-4429</a>
Cisco-application	The installation component on Cisco Application Policy Infrastructure Controller (APIC) devices with software before 1.3(2f) mishandles binary files, which allows local users to obtain root access via unspecified vectors, aka Bug ID CSCu72347.	09/06/2016	7.2	<a href="#">CVE-2016-1430</a>
Medhotos-periperative	MEDHOST Periperative Information Management System (aka PIMS or VPMS) before 2015R3 has hardcoded credentials, which makes it easier for remote attackers to obtain sensitive information via direct requests to the application database server.	09/06/2016	10.0	<a href="#">CVE-2016-4128</a>
Chef-chef	The Chef Manage (formerly opscode-manage) add-on before 1.12.0 for Chef allows remote attackers to execute arbitrary code via crafted serialized data in a cookie.	09/06/2016	7.5	<a href="#">CVE-2016-4126</a>
Emc-networker	EMC NetWorker 8.2.1.x and 8.2.2.x before 8.2.2.6 and 9.x before 9.0.0.6 mishandles authentication, which allows remote attackers to execute arbitrary commands by leveraging access to a different NetWorker instance.	09/06/2016	10.0	<a href="#">CVE-2016-0916</a>
Xinsoft-libeml	Format string vulnerability in libeml before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.	09/06/2016	10.0	<a href="#">CVE-2016-4448</a>
Redhat-enterprise	The smardart interaction in SPICE allows remote attackers to cause a denial of service (QEMU-KVM process crash) or possibly execute arbitrary code via vectors related to connecting to a guest VM, which triggers a heap-based buffer overflow.	09/06/2016	10.0	<a href="#">CVE-2016-0749</a>
Ge-multilink	General Electric (GE) Multilink ML300, ML1200, ML1600, and ML2400 switches with firmware before 5.5.0 and ML310, ML300, and ML310 switches with firmware before 5.5.0x have hardcoded credentials, which allows remote attackers to modify configuration settings via the web interface.	09/06/2016	10.0	<a href="#">CVE-2016-2310</a>
Videolan-vlc	Buffer overflow in the <code>DeodeAdpctimaQT</code> function in <code>modules/codecdpccm</code> in VideoLAN VLC media player before 2.2.4 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted QuickTime TMA file.	08/06/2016	7.5	<a href="#">CVE-2016-5108</a>
Redhat-operashift	Red Hat OpenShift Enterprise 3.2 and OpenShift Origin allow remote authenticated users to execute commands with root privileges by changing the root operation in an <code>rbuilder</code> object.	08/06/2016	9.0	<a href="#">CVE-2016-2160</a>
Hp-universalcmb	HP Universal CMDB 10.0 through 10.2, Universal CMDB Configuration Manager 10.0 through 10.21, and Universal Discovery 10.0 through 10.21 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	08/06/2016	7.5	<a href="#">CVE-2016-4168</a>
Hp-systems insight manager	HP Systems Insight Manager (SIM) before 7.5.1 allows remote attackers to obtain sensitive information, modify data, or cause a denial of service via unspecified vectors.	08/06/2016	7.5	<a href="#">CVE-2016-4466</a>
Hp-insight control server	HP Insight Control server deployment allows local users to gain privileges via unspecified vectors.	08/06/2016	7.5	<a href="#">CVE-2016-4464</a>
Hp-performance center	HP LoadRunner 11.52 through patch 3, 12.00 through patch 3, 12.01 through patch 3, 12.02 through patch 2, and 12.50 through patch 3 and Performance Center 11.52 through patch 1, 12.01 through patch 3, 12.20 through patch 2, and 12.30 through patch 3 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unspecified vectors, aka <a href="#">ZDI-CAN-5916</a> .	08/06/2016	7.5	<a href="#">CVE-2016-4399</a>
Hp-systems insight manager	HP Matrix Operating Environment before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than <a href="#">CVE-2016-2078</a> .	08/06/2016	7.5	<a href="#">CVE-2016-4347</a>
Hp-insight	HP Insight Control before 7.5.1 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unspecified vectors.	08/06/2016	7.5	<a href="#">CVE-2016-2024</a>
Hp-systems insight manager	HP Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than <a href="#">CVE-2016-2017</a> , <a href="#">CVE-2016-2019</a> , <a href="#">CVE-2016-2020</a> , <a href="#">CVE-2016-2021</a> , and <a href="#">CVE-2016-2030</a> .	08/06/2016	7.2	<a href="#">CVE-2016-2021</a>
Hp-systems insight manager	HP Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than <a href="#">CVE-2016-2017</a> , <a href="#">CVE-2016-2019</a> , <a href="#">CVE-2016-2020</a> , <a href="#">CVE-2016-2021</a> , and <a href="#">CVE-2016-2030</a> .	08/06/2016	8.5	<a href="#">CVE-2016-2020</a>
Hp-systems insight manager	HP Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than <a href="#">CVE-2016-2017</a> , <a href="#">CVE-2016-2020</a> , <a href="#">CVE-2016-2021</a> , <a href="#">CVE-2016-2022</a> , and <a href="#">CVE-2016-2030</a> .	08/06/2016	7.2	<a href="#">CVE-2016-2022</a>
Cisco-aironet	Cisco Aironet Access Point Software 8.2(100.0) on 1830e, 1830d, 1850e, 1850d, 2800, and 3800 access points allows local users to obtain Linux root access via crafted <code>cli</code> command parameters, aka Bug ID CSCu64037.	08/06/2016	7.2	<a href="#">CVE-2016-1418</a>
Symantec-data	Directory traversal vulnerability in the Management Server in Symantec Embedded Security: Critical System Protection (SECS/SP) 1.0.x before 1.0 MP1, Embedded Security: Critical System Protection for Controllers and Devices (SECS/SP) 6.5.0 before MP1, Critical System Protection (SCP) before 5.2.9 MP6, Data Center Security: Server Advanced Server (DCS/SA) 6.x before 6.5 MP1 and 6.x before MP1, and Data Center Security: Server Advanced Server and Agents (DCS/SA) through 6.6 MP1 allows remote authenticated users to write update package data to arbitrary agent locations via unspecified vectors.	08/06/2016		<a href="#">CVE-2015-8799</a>
Symantec-data	Directory traversal vulnerability in the Management Server in Symantec Embedded Security: Critical System Protection (SECS/SP) 1.0.x before 1.0 MP1, Embedded Security: Critical System Protection for Controllers and Devices (SECS/SP) 6.5.0 before MP1, Critical System Protection (SCP) before 5.2.9 MP6, Data Center Security: Server Advanced Server (DCS/SA) 6.x before 6.5 MP1 and 6.x before MP1, and Data Center Security: Server Advanced Server and Agents (DCS/SA) through 6.6 MP1 allows remote authenticated users to execute arbitrary code via unspecified vectors.	08/06/2016	7.7	<a href="#">CVE-2015-8798</a>
Apache-Struts	Apache Struts 2.3.20.x before 2.3.20.3, 2.3.24.x before 2.3.24.3, and 2.3.28.x before 2.3.28.1, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via vectors related to an (exclamation mark) operator to the REST plugin.	07/06/2016	7.5	<a href="#">CVE-2016-3087</a>
Debian-linux	The <code>tl1_parse_font_matrix</code> function in <code>type1/t1load.c</code> , <code>(2) tld_parse_font_matrix</code> function in <code>cid/cidload.c</code> , <code>(3) t42_parse_font_matrix</code> function in <code>type42/t42parse.c</code> , and <code>(4) ps_parser_load_field</code> function in <code>psaux/psobj.c</code> in FreeType before 2.5.4 do not check return values, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted font.	07/06/2016	7.5	<a href="#">CVE-2014-9746</a>
Debian-linux	The PDO adapters in Zend Framework before 1.12.16 do not filter null bytes in SQL statements, which allows remote attackers to execute arbitrary SQL commands via a crafted query.	07/06/2016	7.5	<a href="#">CVE-2015-7095</a>
Apache-james	Apache James Server 2.3.2, when configured with file-based user repositories, allows attackers to execute arbitrary system commands via unspecified vectors.	07/06/2016	9.8	<a href="#">CVE-2015-7611</a>
Zend-cache	Doctrine Annotations before 1.2.7, Cache before 1.3.2 and 1.4.x before 1.4.2, Common before 2.4.3 and 2.5.x before 2.5.1, DRM before 2.4.8 or 2.5.x before 2.5.1, MongoDB ODM before 1.0.2, and MongoDB ODM bundle before 10.1 use world-writable permissions for cache directories, which allows local users to execute arbitrary PHP code with additional privileges by leveraging an application with the <code>umask</code> set to 0 and that executes cache entries as code.	07/06/2016	7.8	<a href="#">CVE-2015-5723</a>
redhat-enterprise	Heap-based buffer overflow in SPICE before 0.12.6 allows guest OS users to cause a denial of service (heap-based memory corruption and QEMU-KVM crash) or possibly execute arbitrary code on the host via QXL commands related to the <code>surface_id</code> parameter.	07/06/2016	7.2	<a href="#">CVE-2015-5140</a>
Criu-criu	The <code>service</code> daemon in CRUI creates log and dump files insecurely, which allows local users to create arbitrary files and take ownership of existing files via unspecified vectors related to a directory path.	07/06/2016	7.2	<a href="#">CVE-2015-5128</a>