Histórico de vulnerabilidades de Decembro do 2016

Semana 26/12/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
s9y -- serendipity	include/functions_installer.inc.php in Serendipity through 2.0.5 is vulnerable to File Inclusion and a possible Code Execution attack during a first-time installation because it fails to sanitize the dbType POST parameter before adding it to an include() call in the bundled-libs/serendipity_generateFTPChecksums.php file.	30/12/2016	7.5	CVE-2016-10082
hp -- thinpro	HP ThinPro 4.4 through 6.1 mishandles the keyboard layout control panel and virtual keyboard application, which allows local users to bypass intended access restrictions and gain privileges via unspecified vectors.	29/12/2016	7.2	CVE-2016-2246
pivotal_software -- rabbitmq	An issue was discovered in Pivotal RabbitMQ 3.x before 3.5.8 and 3.6.x before 3.6.6 and RabbitMQ for PCF 1.5.x before 1.5.20, 1.6.x before 1.6.12, and 1.7.x before 1.7.7. MQTT (MQ Telemetry Transport) connection authentication with a username/password pair succeeds if an existing username is provided but the password is omitted from the connection request. Connections that use TLS with a client-provided certificate are not affected.	29/12/2016	7.5	CVE-2016-9877
shutter-project -- shutter	/usr/bin/shutter in Shutter through 0.93.1 allows user-assisted remote attackers to execute arbitrary commands via a crafted image name that is mishandled during a "Run a plugin" action.	29/12/2016	9.3	CVE-2016-10081
vmware -- workstation_pro	Untrusted search path vulnerability in the installer in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows allows local users to gain privileges via a Trojan horse DLL in an unspecified directory.	29/12/2016	7.2	CVE-2016-7085
vmware -- workstation_pro	The installer in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows allows local users to gain privileges via a Trojan horse setup64.exe file in the installation directory.	29/12/2016	7.2	CVE-2016-7086
vmware -- vsphere_data_protection	VMware vSphere Data Protection (VDP) 5.5.x though 6.1.x has an SSH private key with a publicly known password, which makes it easier for remote attackers to obtain login access via an SSH session.	29/12/2016	10.0	CVE-2016-7456
vmware -- vrealize_operations	VMware vRealize Operations (aka vROps) 6.x before 6.4.0 allows remote authenticated users to gain privileges, or halt and remove virtual machines, via unspecified vectors.	29/12/2016	8.0	CVE-2016-7457
vmware -- fusion_pro	The drag-and-drop (aka DnD) function in VMware Workstation Pro 12.x before 12.5.2 and VMware Workstation Player 12.x before 12.5.2 and VMware Fusion and Fusion Pro 8.x before 8.5.2 allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (out-of-bounds memory access on the host OS) via unspecified vectors.	29/12/2016	7.2	CVE-2016-7461
vmware -- vrealize_operations	The Suite REST API in VMware vRealize Operations (aka vROps) 6.x before 6.4.0 allows remote authenticated users to write arbitrary content to files or rename files via a crafted DiskFileItem in a relay-request payload that is mishandled during deserialization.	29/12/2016	7.5	CVE-2016-7462
linux -- linux_kernel	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 3.5 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUF or (2) SO_RCVBUF option.	28/12/2016	7.2	CVE-2012-6704
linux -- linux_kernel	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device.	28/12/2016	7.2	CVE-2016-9576
linux -- linux_kernel	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.	28/12/2016	7.2	CVE-2016-9793
linux -- linux_kernel	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated.	28/12/2016	7.2	CVE-2016-9806
cisco -- cloudcenter_orchestrator	A vulnerability in the Docker Engine configuration of Cisco CloudCenter Orchestrator (CCO; formerly CliQr) could allow an unauthenticated, remote attacker to install Docker containers with high privileges on the affected system. Affected Products: This vulnerability affect all releases of Cisco CloudCenter Orchestrator (CCO) deployments where the Docker Engine TCP port 2375 is open on the system and bound to local address 0.0.0.0 (any interface).	26/12/2016	10.0	CVE-2016-9223
modx -- modx_revolution	Directory traversal in /connectors/index.php in MODX Revolution before 2.5.2-pl allows remote attackers to perform local file inclusion/traversal/manipulation via a crafted id (aka dir) parameter, related to browser/directory/getlist.	24/12/2016	7.5	CVE-2016-10037
modx -- modx_revolution	Directory traversal in /connectors/index.php in MODX Revolution before 2.5.2-pl allows remote attackers to perform local file inclusion/traversal/manipulation via a crafted dir parameter, related to browser/directory/remove.	24/12/2016	7.5	CVE-2016-10038
modx -- modx_revolution	Directory traversal in /connectors/index.php in MODX Revolution before 2.5.2-pl allows remote attackers to perform local file inclusion/traversal/manipulation via a crafted dir parameter, related to browser/directory/getfiles.	24/12/2016	7.5	CVE-2016-10039
debian -- debian_linux	Through a malicious URL that contained a quote character it was possible to inject HTML code in KMail's plaintext viewer. Due to the parser used on the URL it was not possible to include the equal sign (=) or a space into the injected HTML, which greatly reduces the available HTML functionality. Although it is possible to include an HTML comment indicator to hide content.	23/12/2016	7.5	CVE-2016-7966
kde -- kmail	KMail since version 5.3.0 used a QWebEngine based viewer that had JavaScript enabled. HTML Mail contents were not sanitized for JavaScript and included code was executed.	23/12/2016	7.5	CVE-2016-7968
tarantool -- tarantool	An exploitable out-of-bounds array access vulnerability exists in the xrow_header_decode function of Tarantool 1.7.2.0-g8e92715. A specially crafted packet can cause the function to access an element outside the bounds of a global array that is used to determine the type of the specified key's value. This can lead to an out of bounds read within the context of the server. An attacker who exploits this vulnerability can cause a denial of service vulnerability on the server.	23/12/2016	7.8	CVE-2016-9037

Semana 19/12/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bundler -- bundler	Bundler 1.x might allow remote attackers to inject arbitrary Ruby code into an application by leveraging a gem name collision on a secondary source. NOTE: this might overlap CVE-2013-0334.	22/12/2016	7.5	CVE-2016-7954
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."	20/12/2016	7.6	CVE-2016-7181
microsoft -- windows_server_2008	The Graphics Component in the kernel-mode drivers 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, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	20/12/2016	7.2	CVE-2016-7259
microsoft -- windows_server_2008	The kernel-mode drivers 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, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	20/12/2016	7.2	CVE-2016-7260
microsoft -- excel_for_mac	Microsoft Excel for Mac 2011 and Excel 2016 for Mac allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	20/12/2016	9.3	CVE-2016-7263
microsoft -- windows_server_2008	The Graphics component 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, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Graphics Remote Code Execution Vulnerability."	20/12/2016	9.3	CVE-2016-7272
microsoft -- windows_10	The Graphics component in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Graphics Remote Code Execution Vulnerability."	20/12/2016	9.3	CVE-2016-7273
microsoft -- windows_server_2008	Uniscribe 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, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Uniscribe Remote Code Execution Vulnerability."	20/12/2016	9.3	CVE-2016-7274
microsoft -- office	Microsoft Office 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016 mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Microsoft Office OLE DLL Side Loading Vulnerability."	20/12/2016	7.2	CVE-2016-7275
microsoft -- office	Microsoft Office 2016 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	20/12/2016	9.3	CVE-2016-7277
microsoft -- internet_explorer	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."	20/12/2016	7.6	CVE-2016-7279
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."	20/12/2016	9.3	CVE-2016-7283
microsoft -- edge	The scripting engines in 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," a different vulnerability than CVE-2016-7288, CVE-2016-7296, and CVE-2016-7297.	20/12/2016	7.6	CVE-2016-7286
microsoft -- edge	The scripting engines in Microsoft Internet Explorer 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."	20/12/2016	7.6	CVE-2016-7287
microsoft -- edge	The scripting engines in 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," a different vulnerability than CVE-2016-7286, CVE-2016-7296, and CVE-2016-7297.	20/12/2016	7.6	CVE-2016-7288
microsoft -- publisher	Microsoft Publisher 2010 SP2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	20/12/2016	9.3	CVE-2016-7289
microsoft -- windows_server_2016	The Installer 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, 1511, and 1607, and Windows Server 2016 mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Windows Installer Elevation of Privilege Vulnerability."	20/12/2016	7.2	CVE-2016-7292
microsoft -- edge	The scripting engines in 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," a different vulnerability than CVE-2016-7286, CVE-2016-7288, and CVE-2016-7297.	20/12/2016	7.6	CVE-2016-7296
microsoft -- edge	The scripting engines in 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," a different vulnerability than CVE-2016-7286, CVE-2016-7288, and CVE-2016-7296.	20/12/2016	7.6	CVE-2016-7297
microsoft -- word_viewer	Microsoft Office 2007 SP3, Office 2010 SP2, Word Viewer, Office for Mac 2011, and Office 2016 for Mac allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	20/12/2016	9.3	CVE-2016-7298
dotcms -- dotcms	SQL injection vulnerability in the REST API in dotCMS before 3.3.2 allows remote attackers to execute arbitrary SQL commands via the stName parameter to api/content/save/1.	19/12/2016	7.5	CVE-2016-2355
blackberry -- good_enterprise_mobility_server	A remote shell execution vulnerability in the BlackBerry Good Enterprise Mobility Server (GEMS) implementation of the Apache Karaf command shell in GEMS versions 2.1.5.3 to 2.2.22.25 allows remote attackers to obtain local administrator rights on the GEMS server via commands executed on the Karaf command shell.	16/12/2016	8.5	CVE-2016-3129
canonical -- ubuntu_linux	An issue was discovered in Apport before 2.20.4. In apport/ui.py, Apport reads the CrashDB field and it then evaluates the field as Python code if it begins with a "{". This allows remote attackers to execute arbitrary Python code.	16/12/2016	9.3	CVE-2016-9949
canonical -- ubuntu_linux	An issue was discovered in Apport before 2.20.4. There is a path traversal issue in the Apport crash file "Package" and "SourcePackage" fields. These fields are used to build a path to the package specific hook files in the /usr/share/apport/package-hooks/ directory. An attacker can exploit this path traversal to execute arbitrary Python files from the local system.	16/12/2016	9.3	CVE-2016-9950
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where multiple pointers are used without checking for NULL, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8813
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where multiple pointers are used without checking for NULL, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8814
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a value passed from a user to the driver is used without validation as the index to an array, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8815
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a value passed from a user to the driver is used without validation as the index to an array, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8816

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a value passed from a user to the driver is used without validation as the size input to memcpy(), causing a buffer overflow, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8817
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a pointer passed from a user to the driver is used without validation, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8818
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a handle to a kernel object may be returned to the user, leading to possible denial of service or escalation of privileges.	16/12/2016	7.2	CVE-2016-8819
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler for DxgDdiEscape where improper access controls may allow a user to access arbitrary physical memory, leading to an escalation of privileges.	16/12/2016	7.2	CVE-2016-8821
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x600000E, 0x600000F, and 0x6000010 where a value passed from a user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8822
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler for DxgDdiEscape where the size of an input buffer is not validated leading to a denial of service or possible escalation of privileges	16/12/2016	7.2	CVE-2016-8823
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where improper access controls allow a regular user to write a part of the registry intended for privileged users only, leading to escalation of privileges.	16/12/2016	7.2	CVE-2016-8824
nvidia -- gpu_driver	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where the size of an input buffer is not validated, leading to denial of service or potential escalation of privileges.	16/12/2016	7.2	CVE-2016-8825
samsung -- samsung_mobile	Lack of appropriate exception handling in some receivers of the Telecom application on Samsung Note devices with L(5.0/5.1), M(6.0), and N(7.0) software allows attackers to crash the system easily resulting in a possible DoS attack, or possibly gain privileges. The Samsung ID is SVE-2016-7119.	16/12/2016	10.0	CVE-2016-9965
samsung -- samsung_mobile	Lack of appropriate exception handling in some receivers of the Telecom application on Samsung Note devices with L(5.0/5.1), M(6.0), and N(7.0) software allows attackers to crash the system easily resulting in a possible DoS attack, or possibly gain privileges. The Samsung ID is SVE-2016-7120.	16/12/2016	10.0	CVE-2016-9966
samsung -- samsung_mobile	Lack of appropriate exception handling in some receivers of the Telecom application on Samsung Note devices with L(5.0/5.1), M(6.0), and N(7.0) software allows attackers to crash the system easily resulting in a possible DoS attack, or possibly gain privileges. The Samsung ID is SVE-2016-7121.	16/12/2016	10.0	CVE-2016-9967
siemens -- simatic_s7-300_cpu_firmware	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs (all versions including V3.2.12) and SIMATIC S7-400 PN CPUs (V6 and V7) could allow a remote attacker to cause a Denial of Service condition by sending specially crafted packets to port 80/TCP.	16/12/2016	7.8	CVE-2016-9158
technicolor -- xfinity_gateway_router_dpc3941t_firmware	CSRF vulnerability on Technicolor TC dpc3941T (formerly Cisco dpc3941T) devices with firmware dpc3941-P20-18-v303r20421733-160413a-CMCST allows an attacker to change the Wi-Fi password, open the remote management interface, or reset the router.	16/12/2016	7.9	CVE-2016-7454

Semana 12/12/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
samsung -- samsung_mobile	Lack of appropriate exception handling in some receivers of the Telecom application on Samsung Note devices with L(5.0/5.1), M(6.0), and N(7.0) software allows attackers to crash the system easily resulting in a possible DoS attack, or possibly gain privileges. The Samsung ID is SVE-2016-7119.	16/12/2016	10.0	CVE-2016-9965
samsung -- samsung_mobile	Lack of appropriate exception handling in some receivers of the Telecom application on Samsung Note devices with L(5.0/5.1), M(6.0), and N(7.0) software allows attackers to crash the system easily resulting in a possible DoS attack, or possibly gain privileges. The Samsung ID is SVE-2016-7120.	16/12/2016	10.0	CVE-2016-9966
samsung -- samsung_mobile	Lack of appropriate exception handling in some receivers of the Telecom application on Samsung Note devices with L(5.0/5.1), M(6.0), and N(7.0) software allows attackers to crash the system easily resulting in a possible DoS attack, or possibly gain privileges. The Samsung ID is SVE-2016-7121.	16/12/2016	10.0	CVE-2016-9967
adobe -- dng_converter	Adobe DNG Converter versions 9.7 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7856
adobe -- animate	Adobe Animate versions 15.2.1.95 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7866
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to bookmarking in searches. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7867
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to alternation functionality. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7868
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to backtrack search functionality. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7869
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class for specific search strategies. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7870
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the Worker class. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7871
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the MovieClip class related to objects at multiple presentation levels. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7872
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the PSDK class related to ad policy functionality method. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7873
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the NetConnection class when handling the proxy types. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7874
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable integer overflow vulnerability in the BitmapData class. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7875
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the Clipboard class related to data handling functionality. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7876
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the Action Message Format serialization (AFM0). Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7877
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the PSDK's MediaPlayer class. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7878
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the NetConnection class when handling an attached script object. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7879
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability when setting the length property of an array object. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7880
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the MovieClip class when handling conversion to an object. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7881
adobe -- indesign	Adobe InDesign version 11.4.1 and earlier, Adobe InDesign Server 11.0.0 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7886
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have security bypass vulnerability in the implementation of the same origin policy.	15/12/2016	7.5	CVE-2016-7890
adobe -- flash_player	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the TextField class. Successful exploitation could lead to arbitrary code execution.	15/12/2016	10.0	CVE-2016-7892
nagios -- nagios	MagpieRSS, as used in the front-end component in Nagios Core before 4.2.2 might allow remote attackers to read or write to arbitrary files by spoofing a crafted response from the Nagios RSS feed server. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4796.	15/12/2016	7.5	CVE-2016-9565
nagios -- nagios	base/logging.c in Nagios Core before 4.2.4 allows local users with access to an account in the nagios group to gain root privileges via a symlink attack on the log file. NOTE: this can be leveraged by remote attackers using CVE-2016-9565.	15/12/2016	7.2	CVE-2016-9566
joyent -- smartos	An exploitable integer overflow exists in the Joyent SmartOS 20161110T013148Z Hyprlofs file system. The vulnerability is present in the Ioctl system call with the command HYPRLOFS_ADD_ENTRIES when dealing with native file systems. An attacker can craft an input that can cause a kernel panic and potentially be leveraged into a full privilege escalation vulnerability. This vulnerability is distinct from CVE-2016-9031.	14/12/2016	7.2	CVE-2016-8733
mailcwp_project -- mailcwp	Mailcwp remote file upload vulnerability incomplete fix v1.100	14/12/2016	7.5	CVE-2016-1000156
redhat -- enterprise_linux_server	XRegion in TigerVNC allows remote VNC servers to cause a denial of service (NULL pointer dereference) by leveraging failure to check a malloc return value, a similar issue to CVE-2014-6052.	14/12/2016	7.5	CVE-2014-8241
7-zip -- 7-zip	Heap-based buffer overflow in the NArchive::NHfs::CHandler::ExtractZlibFile method in 7zip before 16.00 and p7zip allows remote attackers to execute arbitrary code via a crafted HFS+ image.	13/12/2016	9.3	CVE-2016-2334
bmc -- bladelogic_server_automation_console	BMC BladeLogic Server Automation (BSA) before 8.7 Patch 3 allows remote attackers to bypass authentication and consequently read arbitrary files or possibly have unspecified other impact by leveraging a "logic flaw" in the authentication process.	13/12/2016	7.5	CVE-2016-4322
cisco -- hybrid_media_service	A vulnerability in the installation procedure of the Cisco Hybrid Media Service could allow an authenticated, local attacker to elevate privileges to the root level. More Information: CSCvb81344. Known Affected Releases: 1.0.	13/12/2016	7.2	CVE-2016-6470
cisco -- anyconnect_secure_mobility_client	A vulnerability in Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and execute an arbitrary executable file with privileges equivalent to the Microsoft Windows operating system SYSTEM account. More Information: CSCvb68043. Known Affected Releases: 4.3(2039) 4.3(748). Known Fixed Releases: 4.3(4019) 4.4(225).	13/12/2016	7.2	CVE-2016-9192
cisco -- ios_xr	A vulnerability in Cisco IOS XR Software could allow an authenticated, local attacker to log in to the device with the privileges of the root user. More Information: CSCva38434. Known Affected Releases: 6.1.1.BASE.	13/12/2016	7.2	CVE-2016-9215
fedoraproject -- fedora	The (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXv before 1.0.11 allow remote X servers to trigger out-of-bounds memory access operations via vectors involving length specifications in received data.	13/12/2016	7.5	CVE-2016-5407
fedoraproject -- fedora	The XGetImage function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving image type and geometry, which triggers out-of-bounds read operations.	13/12/2016	7.5	CVE-2016-7942
fedoraproject -- fedora	The XListFonts function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving length fields, which trigger out-of-bounds write operations.	13/12/2016	7.5	CVE-2016-7943
fedoraproject -- fedora	Integer overflow in X.org libXfixes before 5.0.3 on 32-bit platforms might allow remote X servers to gain privileges via a length value of INT_MAX, which triggers the client to stop reading data and get out of sync.	13/12/2016	7.5	CVE-2016-7944
fedoraproject -- fedora	Multiple integer overflows in X.org libXrandr before 1.5.1 allow remote X servers to trigger out-of-bounds write operations via a crafted response.	13/12/2016	7.5	CVE-2016-7947
fedoraproject -- fedora	X.org libXrandr before 1.5.1 allows remote X servers to trigger out-of-bounds write operations by leveraging mishandling of reply data.	13/12/2016	7.5	CVE-2016-7948
fedoraproject -- fedora	Multiple buffer overflows in the (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXrender before 0.9.10 allow remote X servers to trigger out-of-bounds write operations via vectors involving length fields.	13/12/2016	7.5	CVE-2016-7949
fedoraproject -- fedora	The XRenderQueryFilters function in X.org libXrender before 0.9.10 allows remote X servers to trigger out-of-bounds write operations via vectors involving filter name lengths.	13/12/2016	7.5	CVE-2016-7950
fedoraproject -- fedora	Multiple integer overflows in X.org libXtst before 1.2.3 allow remote X servers to trigger out-of-bounds memory access operations by leveraging the lack of range checks.	13/12/2016	7.5	CVE-2016-7951
fedoraproject -- fedora	Buffer underflow in X.org libXvMC before 1.0.10 allows remote X servers to have unspecified impact via an empty string.	13/12/2016	7.5	CVE-2016-7953
google -- android	A remote code execution vulnerability in libstagefright in Mediaserver in Android 7.0 before 2016-11-01 could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Android ID: A-31373622.	13/12/2016	9.3	CVE-2016-6699
google -- android	An elevation of privilege vulnerability in libstagefright in Mediaserver in Android 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A-31385713.	13/12/2016	9.3	CVE-2016-6706

Histórico de vulnerabilidades de Decembro do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	A remote denial of service vulnerability in libvpx 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 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-30593765.	13/12/2016	7.1	CVE-2016-6711
google -- android	A remote denial of service vulnerability in libvpx 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 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-30593752.	13/12/2016	7.1	CVE-2016-6712
oracle -- solaris	The VerticalFilter function in the DDS coder in ImageMagick before 6.9.4-3 and 7.x before 7.0.1-4 allows remote attackers to have unspecified impact via a crafted DDS file, which triggers an out-of-bounds read.	13/12/2016	7.5	CVE-2016-5687
oracle -- solaris	The DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact by leveraging lack of NULL pointer checks.	13/12/2016	7.5	CVE-2016-5689
oracle -- solaris	The ReadDCMImage function in DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact via vectors involving the for statement in computing the pixel scaling table.	13/12/2016	7.5	CVE-2016-5690
oracle -- solaris	The DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact by leveraging lack of validation of (1) pixel.red, (2) pixel.green, and (3) pixel.blue.	13/12/2016	7.5	CVE-2016-5691
oracle -- solaris	Integer overflow in MagickCore/profile.c in ImageMagick before 7.0.2-1 allows remote attackers to cause a denial of service (segmentation fault) or possibly execute arbitrary code via vectors involving the offset variable.	13/12/2016	7.5	CVE-2016-5841
pcre -- pcre	Heap-based buffer overflow in PCRE 8.34 through 8.37 and PCRE2 10.10 allows remote attackers to execute arbitrary code via a crafted regular expression, as demonstrated by /^(?P=B)((?P=B)(?J:(?P<B>c)(?P<B>a(?P=B)))>WGXCREDITS)/, a different vulnerability than CVE-2015-8384.	13/12/2016	7.5	CVE-2015-3210
bdwgc_project -- bdwgc	Integer overflow vulnerability in bdwgc before 2016-09-27 allows attackers to cause client of bdwgc denial of service (heap buffer overflow crash) and possibly execute arbitrary code via huge allocation.	11/12/2016	7.5	CVE-2016-9427
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin. Some data is passed to the PHP unserialize() function without verification that it's valid serialized data. The unserialization can result in code execution because of the interaction with object instantiation and autoloading. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	10/12/2016	7.5	CVE-2016-6620
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin involving the $cfg['ArbitraryServerRegexp'] configuration directive. An attacker could reuse certain cookie values in a way of bypassing the servers defined by ArbitraryServerRegexp. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	10/12/2016	10.0	CVE-2016-6629
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin. A user can execute a remote code execution attack against a server when phpMyAdmin is being run as a CGI application. Under certain server configurations, a user can pass a query string which is executed as a command-line argument by the file generator_plugin.sh. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	10/12/2016	8.5	CVE-2016-6631
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin. It is possible to bypass AllowRoot restriction ($cfg['Servers'][$i]['AllowRoot']) and deny rules for username by using Null Byte in the username. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	10/12/2016	7.5	CVE-2016-9849
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin. Due to a bug in serialized string parsing, it was possible to bypass the protection offered by PMA_safeUnserialize() function. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	10/12/2016	7.5	CVE-2016-9865
atlassian -- crowd	The LDAP directory connector in Atlassian Crowd before 2.8.8 and 2.9.x before 2.9.5 allows remote attackers to execute arbitrary code via an LDAP attribute with a crafted serialized Java object, aka LDAP entry poisoning.	09/12/2016	7.5	CVE-2016-6496
busybox -- busybox	The recv_and_process_client_pkt function in networking/ntpd.c in busybox allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged NTP packet, which triggers a communication loop.	09/12/2016	7.8	CVE-2016-6301
crowbar_project -- barclamp-trove	The trove service user in (1) Openstack deployment (aka crowbar-openstack) and (2) Trove Barclamp (aka barclamp-trove and crowbar-barclamp-trove) in the Crowbar Framework has a default password, which makes it easier for remote attackers to obtain access via unspecified vectors.	09/12/2016	7.5	CVE-2016-6829
djangoproject -- django	Django 1.8.x before 1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3 use a hardcoded password for a temporary database user created when running tests with an Oracle database, which makes it easier for remote attackers to obtain access to the database server by leveraging failure to manually specify a password in the database settings TEST dictionary.	09/12/2016	7.5	CVE-2016-9013
jfrog -- artifactory	JFrog Artifactory before 4.11 allows remote attackers to execute arbitrary code via an LDAP attribute with a crafted serialized Java object, aka LDAP entry poisoning.	09/12/2016	7.5	CVE-2016-6501

Semana 05/12/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	arch/arm64/kernel/sys.c in the Linux kernel before 4.0 allows local users to bypass the "strict page permissions" protection mechanism and modify the system-call table, and consequently gain privileges, by leveraging write access.	08/12/2016	9.3	CVE-2015-8967
intel -- wireless_bluetooth_drivers	Unquoted service path vulnerability in Intel Wireless Bluetooth Drivers 16.x, 17.x, and before 18.1.1607.3129 allows local users to launch processes with elevated privileges.	08/12/2016	7.2	CVE-2016-8102
linux -- linux_kernel	arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) F_OFD_GETLK, (2) F_OFD_SETLK, or (3) F_OFD_SETLKW command in an fcntl64 system call.	08/12/2016	7.2	CVE-2015-8966
linux -- linux_kernel	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions.	08/12/2016	7.2	CVE-2016-8655
linux -- linux_kernel	Race condition in the ion_ioctl function in drivers/staging/android/ion/ion.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) by calling ION_IOC_FREE on two CPUs at the same time.	08/12/2016	9.3	CVE-2016-9120
linux -- linux_kernel	The icmp6_send function in net/ipv6/icmp.c in the Linux kernel through 4.8.12 omits a certain check of the dst data structure, which allows remote attackers to cause a denial of service (panic) via a fragmented IPv6 packet.	08/12/2016	7.8	CVE-2016-9919
google -- android	The GPS component in Android before 2016-12-05 allows man-in-the-middle attackers to cause a denial of service (GPS signal-acquisition delay) via an incorrect xtra.bin or xtra2.bin file on a spoofed Qualcomm gpsonextra.net or izatcloud.net host, aka internal bug 31470303 and external bug 211602 (and AndroidID-7225554).	06/12/2016	7.1	CVE-2016-5341
joomla -- joomla!	The file scanning mechanism of JFilterInput::isFileSafe() in Joomla! CMS before 3.6.5 does not consider alternative PHP file extensions when checking uploaded files for PHP content, which enables a user to upload and execute files with the \`.php6\`, \`.php7\`, \`.phtml\`, and \`.phpt\` extensions. Additionally, JHelperMedia::canUpload() did not blacklist these file extensions as uploadable file types.	05/12/2016	7.5	CVE-2016-9836
siemens -- sicam_pas	A vulnerability in Siemens SICAM PAS (all versions including V8.08) could allow a remote attacker to upload, download, or delete files in certain parts of the file system by sending specially crafted packets to port 19235/TCP.	05/12/2016	7.5	CVE-2016-9156
siemens -- sicam_pas	A vulnerability in Siemens SICAM PAS (all versions including V8.08) could allow a remote attacker to cause a Denial of Service condition and potentially lead to unauthenticated remote code execution by sending specially crafted packets sent to port 19234/TCP.	05/12/2016	7.5	CVE-2016-9157
zikula -- zikula_application_framework	Directory traversal vulnerability in file "jcss.php" in Zikula 1.3.x before 1.3.11 and 1.4.x before 1.4.4 on Windows allows a remote attacker to launch a PHP object injection by uploading a serialized file.	05/12/2016	7.5	CVE-2016-9835
alcatel-lucent -- omnivista_8770_network_management_system	Alcatel-Lucent OmniVista 8770 2.0 through 3.0 exposes different ORBs interfaces, which can be queried using the GIOP protocol on TCP port 30024. An attacker can bypass authentication, and OmniVista invokes methods (AddJobSet, AddJob, and ExecuteNow) that can be used to run arbitrary commands on the server, with the privilege of NT AUTHORITY\SYSTEM on the server. NOTE: The discoverer states "The vendor position is to refer to the technical guidelines of the product security deployment to mitigate this issue, which means applying proper firewall rules to prevent unauthorised clients to connect to the OmniVista server."	03/12/2016	10.0	CVE-2016-9796