Últimas vulnerabilidades

En esta sección se mostrarán de forma mensual las vulnerabilidades de nivel alto más recientes.
Las vulnerabilidades de la tabla están ordenadas cronológicamente descendente.

<>

Semana 20/03/2017

Primary Vendor -- Product	Description	Source
canonical – ubuntu_linux	The ReadPSDLayers function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors, related to "throwing of exceptions."	CVE-2014-9841
canonical – ubuntu_linux	The DecodePSDPixels function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors.	CVE-2014-9843
canonical – ubuntu_linux	Buffer overflow in the ReadRLEImage function in coders/rle.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact.	CVE-2014-9846
canonical – ubuntu_linux	The jng decoder in ImageMagick 6.8.9.9 allows remote attackers to have an unspecified impact.	CVE-2014-9847

cerberus -- cerberus_ftp_server	Buffer overflow in Cerberus FTP Server 8.0.10.3 allows remote attackers to cause a denial of service (daemon crash) or possibly have unspecified other impact via a long MLST command.	CVE-2017-6880
chef_manage_project -- chef_manage	The user-account creation feature in Chef Manage 2.1.0 through 2.4.4 allows remote attackers to execute arbitrary code. This is fixed in 2.4.5.	CVE-2017-7174
erlang -- erlang/otp	An issue was discovered in Erlang/OTP 18.x. Erlang's generation of compiled regular expressions is vulnerable to a heap overflow. Regular expressions using a malformed extpattern can indirectly specify an offset that is used as an array index. This ordinal permits arbitrary regions within the erts_alloc arena to be both read and written to.	CVE-2016-10253
gnu -- binutils	ihex.c in GNU Binutils before 2.26 contains a stack buffer overflow when printing bad bytes in Intel Hex objects.	CVE-2014-9939
gnu -- screen	GNU screen before 4.5.1 allows local users to modify arbitrary files and consequently gain root privileges by leveraging improper checking of logfile permissions.	CVE-2017-5618
ibm -- power_hardware_management_console	IBM Power Hardware Management Console (HMC) 3.3.2 and 4.1 could allow a local user to escalate their privileges to gain root access. IBM Reference #: 1998459.	CVE-2017-1134
ibm -- websphere_mq	IBM WebSphere MQ 8.0.0.6 does not properly terminate channel agents when they are no longer needed, which could allow a user to cause a denial of service through resource exhaustion. IBM Reference #: 1999672.	CVE-2017-1145
imagemagick -- imagemagick	distribute-cache.c in ImageMagick re-uses objects after they have been destroyed, which allows remote attackers to have unspecified impact via unspecified vectors.	CVE-2014-9852
imagemagick -- imagemagick	Memory leak in the NewXMLTree function in magick/xml-tree.c in ImageMagick before 6.9.4-7 allows remote attackers to cause a denial of service (memory consumption) via a crafted XML file.	CVE-2016-10047
imagemagick -- imagemagick	Memory leak in the ReadPSDLayers function in coders/psd.c in ImageMagick before 6.9.6-3 allows remote	CVE-2016-10058

	attackers to cause a denial of service (memory consumption) via a crafted image file.	
juniper – junos_space	Insufficient authentication vulnerability in Junos Space before 15.2R2 allows remote network based users with access to Junos Space web interface to perform certain administrative tasks without authentication.	CVE-2016-4926
juniper – junos_space	Command injection vulnerability in Junos Space before 15.2R2 allows attackers to execute arbitrary code as a root user.	CVE-2016-4929
kinsey – infor-lawson	Multiple SQL injection vulnerabilities in Kinsey Infor-Lawson (formerly ESBUS) allow remote attackers to execute arbitrary SQL commands via the (1) TABLE parameter to esbus/servlet/GetSQLData or (2) QUERY parameter to KK_LS9ReportingPortal/GetData.	CVE-2017-6550
linux – linux_kernel	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.	CVE-2017-7187
netiq – access_governance_suite	A logged-in user in NetIQ Access Governance Suite 6.0 through 6.4 could escalate privileges to administrator.	CVE-2016-1597
netiq – access_manager	iManager Admin Console in NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 was vulnerable to iFrame manipulation attacks, which could allow remote users to gain access to authentication credentials.	CVE-2016-5757
oneplus – oxygenos	An issue was discovered in OxygenOS before 4.1.0 on OnePlus 3 and 3T devices. The attacker can change the bootmode of the device by issuing the 'fastboot oem boot_mode {rf/wlan/ftm/normal} command' in contradiction to the threat model of Android where the bootloader MUST NOT allow any security-sensitive operation to be run unless the bootloader is unlocked.	CVE-2017-5623
openinfosecfoundation – suricata	The MemcmpLowercase function in Suricata before 2.0.6 improperly excludes the first byte from comparisons, which might allow remote attackers to bypass intrusion-prevention functionality via a crafted HTTP request.	CVE-2015-8954
pluck-cms – pluck	Pluck CMS 4.7.2 allows remote attackers to execute arbitrary code via the blog form feature.	CVE-2014-8708
qdpm – qdpm	Unrestricted file upload vulnerability in the (1) myAccount, (2) projects, (3) tasks, (4) tickets, (5) discussions, (6) reports, and (7) scheduler pages in qdPM 8.3 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in uploads/attachments/ or uploads/users/.	CVE-2015-3884
wondercms – wondercms	Directory traversal vulnerability in index.php in Wonder CMS 2014 allows remote attackers to include and execute arbitrary local files via a crafted theme.	CVE-2014-8704
wondercms – wondercms	PHP remote file inclusion vulnerability in editInplace.php in Wonder CMS 2014 allows remote attackers to execute arbitrary PHP code via a URL in the hook parameter.	CVE-2014-8705
xrdp – xrdp	xrdp 0.9.1 calls the PAM function auth_start_session() in an incorrect location, leading to PAM session modules	CVE-2017-6967

not being properly initialized, with a potential consequence of incorrect configurations or elevation of privileges, aka a pam_limits.so bypass.