Top / most probable CVEs on systems

**Palo alto**

**CVE-2019-1582** - Memory corruption in PAN-OS 8.1.9 and earlier, and PAN-OS 9.0.3 and earlier will allow an administrative user to cause arbitrary memory corruption by rekeying the current client interactive session.

**CVE-2019-1581** - Mitigation bypass in PAN-OS 7.1.24 and earlier, PAN-OS 8.0.19 and earlier, PAN-OS 8.1.9 and earlier, and PAN-OS 9.0.3 and earlier will allow a remote, unauthenticated user to execute arbitrary code by crafting a malicious message.

**CVE-2019-1580** - Memory corruption in PAN-OS 7.1.24 and earlier, PAN-OS 8.0.19 and earlier, PAN-OS 8.1.9 and earlier, and PAN-OS 9.0.3 and earlier will allow a remote, unauthenticated user to craft a message to Secure Shell Daemon (SSHD) and corrupt arbitrary memory.

**CVE-2019-1579** - Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11-h1 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code.

**CVE-2019-1576** - Command injection in PAN-0S 9.0.2 and earlier may allow an authenticated attacker to gain access to a remote shell in PAN-OS, and potentially run with the escalated users permissions.

**CVE-2019-1575** - Information disclosure in PAN-OS 7.1.23 and earlier, PAN-OS 8.0.18 and earlier, PAN-OS 8.1.8-h4 and earlier, and PAN-OS 9.0.2 and earlier may allow for an authenticated user with read-only privileges to extract the API key of the device and/or the username/password from the XML API (in PAN-OS) and possibly escalate privileges granted to them.

**CVE-2019-1572** - PAN-OS 9.0.0 may allow an unauthenticated remote user to access php files.

**CVE-2018-18065** - Set key in agent/helpers/table\_container.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

**CVE-2018-10141** - GlobalProtect Portal Login page in Palo Alto Networks PAN-OS before 8.1.4 allows an unauthenticated attacker to inject arbitrary JavaScript or HTML.

**CVE-2018-10139** - The PAN-OS response for GlobalProtect Gateway in Palo Alto Networks PAN-OS 6.1.21 and earlier, PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11 and earlier may allow an unauthenticated attacker to inject arbitrary JavaScript or HTML. PAN-OS 8.1 is NOT affected.

**Windows 2k8**

**CVE-2011-0661** SMB server service

**CVE-2011-1268** SMB client service

**CVE-2011-2013** Integer overflow

**CVE-2010-025** Heap based buffer overflow in DirectZone

**CVE-2010-0252** Corrupted system state by remote code bring ran

**CVE-2010-0811** Multiple vulnerabilities in IE8 developer tools

**CVE-2010-1883** Integer overflow in EOT

**CVE-2010-2729** Print spooler service allows remote users to create files in system directories

**CVE-2010-3966** When BranchCache is supported, remote users can privileges by a Trojan horse dll.

**Ubuntu**

**CVE-2019-18634** In Sudo before 1.8.26, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. (pwfeedback is a default setting in Linux Mint and elementary OS; however, it is NOT the default for upstream and many other packages, and would exist only if enabled by an administrator.) The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c.

**Centos**

**CVE-2017-1000253** Overflow; the entire binary which means that, while the first PT\_LOAD segment is mapped below mm->mmap\_base, the subsequent PT\_LOAD segment(s) end up being mapped above mm->mmap\_base into the are that is supposed to be the "gap" between the stack and the binary.

CVE-2011-4144 Unspecified vulnerability in EMC Documentum Content Server 6.0, 6.5 before SP2 P02, 6.5 SP3 before SP3 P02, and 6.6 before P02 allows local users to obtain "highest super user privileges" by leveraging system administrator privileges.

**Fedora**

**CVE-2014-0247** LibreOffice 4.2.4 executes unspecified VBA macros automatically, which has unspecified impact and attack vectors, possibly related to doc/docmacromode.cxx.

**CVE-2014-1519** Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

**CVE-2014-1522** The mozilla::dom::OscillatorNodeEngine::ComputeCustom function in the Web Audio subsystem in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read, memory corruption, and application crash) via crafted content.

**CVE-2014-1528** The sse2\_composite\_src\_x888\_8888 function in Pixman, as used in Cairo in Mozilla Firefox 28.0 and SeaMonkey 2.25 on Windows, allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write and application crash) by painting on a CANVAS element.

**CVE-2015-0278** libuv before 0.10.34 does not properly drop group privileges, which allows context-dependent attackers to gain privileges via unspecified vectors.

**CVE-2015-1815** The get\_rpm\_nvr\_by\_file\_path\_temporary function in util.py in setroubleshoot before 3.2.22 allows remote attackers to execute arbitrary commands via shell metacharacters in a file name.

**CVE-2015-2806** Stack-based buffer overflow in asn1\_der\_decoding in libtasn1 before 4.4 allows remote attackers to have an unspecified impact via unknown vectors.

**CVE-2015-6855** hw/ide/core.c in QEMU does not properly restrict the commands accepted by an ATAPI device, which allows guest users to cause a denial of service or possibly have unspecified other impact via certain IDE commands, as demonstrated by a WIN\_READ\_NATIVE\_MAX command to an empty drive, which triggers a divide-by-zero error and instance crash.

**CVE-2015-7201** Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

**CVE-2015-7202** Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 43.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

**CVE-2015-7203** Buffer overflow in the DirectWriteFontInfo::LoadFontFamilyData function in gfx/thebes/gfxDWriteFontList.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted font-family name.

**CVE-2015-7205** Integer underflow in the RTPReceiverVideo::ParseRtpPacket function in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 might allow remote attackers to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a crafted WebRTC RTP packet.

**CVE-2015-7220** Buffer overflow in the XDRBuffer::grow function in js/src/vm/Xdr.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.

**Windows 8.1**

**CVE-2019-1359** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1358.

**CVE-2019-1347** A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1343, CVE-2019-1346.

**CVE-2019-1342** An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1315, CVE-2019-1339.

**CVE-2019-1333** A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.

**CVE-2019-1341** An elevation of privilege vulnerability exists when umpo.dll of the Power Service, improperly handles a Registry Restore Key function, aka 'Windows Power Service Elevation of Privilege Vulnerability'.

**CVE-2019-1181** A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services? Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1182, CVE-2019-1222, CVE-2019-1226.

**CVE-2019-1183** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'.

**CVE-2019-1280** A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.

**CVE-2019-1212** A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets, aka 'Windows DHCP Server Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1206.

**CVE-2019-1236** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208.

**OScommerce**

CVE-2011-4543Multiple directory traversal vulnerabilities in osCommerce 3.0.2 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) set or (2) module parameter to OM/Core/Site/Admin/Application/templates\_modules\_layout/pages/main.php, (13) OM/Core/Site/Admin/Application/templates\_modules\_layout/pages/new.php, or (14) OM/Core/Site/Admin/Application/templates\_modules\_layout/pages/edit.php; or the template parameter to (15) OM/Core/Site/Admin/Application/templates/pages/info.php, (16) OM/Core/Site/Admin/Application/templates/pages/edit.php, or (17) OM/Core/Site/Admin/Application/templates/pages/uninstall.php.

**CVE-2008-0719** SQL injection vulnerability in customer\_testimonials.php in the Customer Testimonials 3 and 3.1 Addon for osCommerce Online Merchant 2.2 allows remote attackers to execute arbitrary SQL commands via the testimonial\_id parameter.

**CVE-2006-6533** Directory traversal vulnerability in admin/templates\_boxes\_layout.php in osCommerce 3.0a3 allows remote attackers to include and execute arbitrary PHP files via a .. (dot dot) in the filter parameter. NOTE: this issue can be leveraged to obtain full path information in error messages.

**CVE-2006-4297** SQL injection vulnerability in shopping\_cart.php in osCommerce before 2.2 Milestone 2 060817 allows remote attackers to execute arbitrary SQL commands via id array parameters.

**CVE-2005-4677** SQL injection vulnerability in additional\_images.php (aka the Additional Images module) before 1.14 in osCommerce allows remote attackers to execute arbitrary SQL commands via the products\_id parameter to product\_info.php.

**CVE-2004-2638** The Admin Access With Levels plugin in osCommerce 1.5.1 allows remote attackers to access files in the "admin/" directory by modifying the in\_login parameter to a non-zero value.

**CVE-2002-2019** PHP remote file inclusion vulnerability in include\_once.php in osCommerce (a.k.a. Exchange Project) 2.1 allows remote attackers to execute arbitrary PHP code via the include\_file parameter.

**CVE-2002-1991** PHP file inclusion vulnerability in osCommerce 2.1 execute arbitrary commands via the include\_file parameter to include\_once.php.

**CVE-2018-18573** osCommerce 2.3.4.1 has an incomplete '.htaccess' for blacklist filtering in the "product" page. Remote authenticated administrators can upload new '.htaccess' files (e.g., omitting .php) and subsequently achieve arbitrary PHP code execution via a /catalog/admin/categories.php?cPath=&action=new\_product URI.

**CVE-2018-18572** osCommerce 2.3.4.1 has an incomplete '.htaccess' for blacklist filtering in the "product" page. Because of this filter, script files with certain PHP-related extensions (such as .phtml and .php5) didn't execute in the application. But this filter didn't prevent the '.pht' extension. Thus, remote authenticated administrators can upload '.pht' files for arbitrary PHP code execution via a /catalog/admin/categories.php?cPath=&action=new\_product URI.

**Docker**

**CVE-2019-5736** runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.

**CVE-2019-15752** Docker Desktop Community Edition before 2.1.0.1 allows local users to gain privileges by placing a Trojan horse docker-credential-wincred.exe file in %PROGRAMDATA%\DockerDesktop\version-bin\ as a low-privilege user, and then waiting for an admin or service user to authenticate with Docker, restart Docker, or run 'docker login' to force the command.

**CVE-2019-14271** In Docker 19.03.x before 19.03.1 linked against the GNU C Library (aka glibc), code injection can occur when the nsswitch facility dynamically loads a library inside a chroot that contains the contents of the container.

**CVE-2014-0048** An issue was found in Docker before 1.6.0. Some programs and scripts in Docker are downloaded via HTTP and then executed or used in unsafe ways.

**CVE-2014-8179** Docker Engine before 1.8.3 and CS Docker Engine before 1.6.2-CS7 does not properly validate and extract the manifest object from its JSON representation during a pull, which allows attackers to inject new attributes in a JSON object and bypass pull-by-digest validation.

**CVE-2014-9356** Path traversal vulnerability in Docker before 1.3.3 allows remote attackers to write to arbitrary files and bypass a container protection mechanism via a full pathname in a symlink in an (1) image or (2) build in a Dockerfile

**Bind**

**CVE-2017-3145** BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named. Affects BIND 9.0.0 to 9.8.x, 9.9.0 to 9.9.11, 9.10.0 to 9.10.6, 9.11.0 to 9.11.2, 9.9.3-S1 to 9.9.11-S1, 9.10.5-S1 to 9.10.6-S1, 9.12.0a1 to 9.12.0rc1.ymlink in an (1) image or (2) build in a Dockerfile

**Roundcube**

**CVE-2008-5619** html2text.php in Chuggnutt HTML to Text Converter, as used in PHPMailer before 5.2.10, RoundCube Webmail (roundcubemail) 0.2-1.alpha and 0.2-3.beta, Mahara, and AtMail Open 1.03, allows remote attackers to execute arbitrary code via crafted input that is processed by the preg\_replace function with the eval switch.

**CVE-2015-2180** The DBMail driver in the Password plugin in Roundcube before 1.1.0 allows remote attackers to execute arbitrary commands via shell metacharacters in the password.

**CVE-2008-562** RoundCube Webmail (roundcubemail) before 0.2-beta allows remote attackers to cause a denial of service (memory consumption) via crafted size parameters that are used to create a large quota image.

**CVE-2013-6172** steps/utils/save\_pref.inc in Roundcube webmail before 0.8.7 and 0.9.x before 0.9.5 allows remote attackers to modify configuration settings via the \_session parameter, which can be leveraged to read arbitrary files, conduct SQL injection attacks, and execute arbitrary code.

**CVE-2009-4076** Cross-site request forgery (CSRF) vulnerability in Roundcube Webmail 0.2.2 and earlier allows remote attackers to hijack the authentication of unspecified users for requests that modify user information via unspecified vectors, a different vulnerability than CVE-2009-4077.

**CVE-2009-4077** Cross-site request forgery (CSRF) vulnerability in Roundcube Webmail 0.2.2 and earlier allows remote attackers to hijack the authentication of unspecified users for requests that send arbitrary emails via unspecified vectors, a different vulnerability than CVE-2009-4076.

**CVE-2014-9587** Multiple cross-site request forgery (CSRF) vulnerabilities in Roundcube Webmail before 1.0.4 allow remote attackers to hijack the authentication of unspecified victims via unknown vectors, related to (1) address book operations or the (2) ACL or (3) Managesieve plugins.

**CVE-2016-4069** Cross-site request forgery (CSRF) vulnerability in Roundcube Webmail before 1.1.5 allows remote attackers to hijack the authentication of users for requests that download attachments and cause a denial of service (disk consumption) via unspecified vectors.

**CVE-2016-4069** In Roundcube from versions 1.2.0 to 1.3.5, with the archive plugin enabled and configured, it's possible to exploit the unsanitized, user-controlled "\_uid" parameter (in an archive.php \_task=mail&\_mbox=INBOX&\_action=plugin.move2archive request) to perform an MX (IMAP) injection attack by placing an IMAP command after a %0d%0a sequence. NOTE: this is less easily exploitable in 1.3.4 and later because of a Same Origin Policy protection mechanism.

**CVE-2015-2181** Multiple buffer overflows in the DBMail driver in the Password plugin in Roundcube before 1.1.0 allow remote attackers to have an unspecified impact via the (1) password or (2) username.

**CVE-2017-8114** Roundcube Webmail allows arbitrary password resets by authenticated users. This affects versions before 1.0.11, 1.1.x before 1.1.9, and 1.2.x before 1.2.5. The problem is caused by an improperly restricted exec call in the virtualmin and sasl drivers of the password plugin.

**CVE-2015-8770** Directory traversal vulnerability in the set\_skin function in program/include/rcmail\_output\_html.php in Roundcube before 1.0.8 and 1.1.x before 1.1.4 allows remote authenticated users with certain permissions to read arbitrary files or possibly execute arbitrary code via a .. (dot dot) in the \_skin parameter to index.php.

**CVE-2016-9920** steps/mail/sendmail.inc in Roundcube before 1.1.7 and 1.2.x before 1.2.3, when no SMTP server is configured and the sendmail program is enabled, does not properly restrict the use of custom envelope-from addresses on the sendmail command line, which allows remote authenticated users to execute arbitrary code via a modified HTTP request that sends a crafted e-mail message.