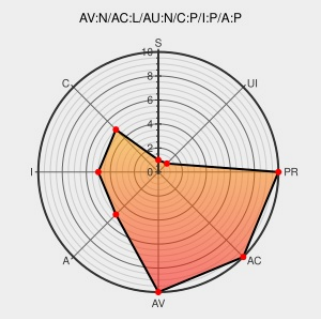
# CVE-2005-2491

Published on: 08/22/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:16:00 AM UTC

## CVE-2005-2491

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Pcre from Pcre contain the following vulnerability:

Integer overflow in pcre_compile.c in Perl Compatible Regular Expressions (PCRE) before 6.2, as used in multiple products such as Python, Ethereal, and PHP, allows attackers to execute arbitrary code via quantifier values in regular expressions, which leads to a heap-based buffer overflow.

CVE-2005-2491 has been assigned by secalert@redhat.com to track the vulnerability

### CVSS2 Score: 7.5 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | www.vupen.com text/html | VUPEN ADV-2006-4320 |
| About Security Update 2005-009 | web.archive.org text/html Inactive Link Not Archived | APPLE APPLE-SA-2005-11-29 |
| Secunia - Advisories - Mac OS X Security Update Fixes Multiple Vulnerabilities | web.archive.org text/html | SECUNIA 17813 |
| PCRE Regular Expression Heap Overflow Vulnerability | cve.report (archive) text/html | BID 14620 |
| Gentoo Linux Documentation -- Gnumeric: Heap overflow in the included PCRE library | www.gentoo.org text/html | GENTOO GLSA-200509-02 |

| | | |
|---|---|---|
| Support | www.redhat.com<br>text/html | REDHAT RHSA-2005:358 |
| Secunia - Advisories - Sun Solaris Multiple Apache2 Vulnerabilities | web.archive.org<br>text/html | SECUNIA 19072 |
| | ftp.sco.com<br>text/plain | SCO SCOSA-2006.10 |
| Avaya Products Integer Overflow and Denial of Service - Secunia Advisories - Vulnerability Intelligence - Secunia.com | web.archive.org<br>text/html | SECUNIA 21522 |
| IT Resource Center - login / register | web.archive.org<br>text/html<br>Inactive Link Not Archived | HP SSRT061238 |
| rhn.redhat.com \| Red Hat Support | www.redhat.com<br>text/html | REDHAT RHSA-2006:0197 |
| SecurityFocus | www.securityfocus.com<br>text/html | HP SSRT051251 |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20210330 svn commit: r1888194 [3/13] - /httpd/site/trunk/content/security/json/ |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20200401 svn commit: r1058586 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | www.vupen.com<br>inode/x-empty | VUPEN ADV-2006-0789 |
| Debian -- Security Information -- DSA-817-1 python2.2 | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-817 |
| Secunia - Advisories - PCRE Quantifier Values Integer Overflow Vulnerability | web.archive.org<br>text/html | SECUNIA 16502 |
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL oval:org.mitre.oval:def:1659 |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20190815 svn commit: r1048742 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| 1. Overview: | support.avaya.com<br>text/html | CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-081.htm |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20210330 svn commit: r1073149 [5/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/ |
| Webmail - OVH | www.vupen.com<br>text/html | VUPEN ADV-2005-1511 |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20200401 svn commit: r1058587 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |

| | | |
|---|---|---|
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20210330 svn commit: r1073140 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohtml.py security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| SecurityFocus | www.securityfocus.com<br>text/html | FEDORA FLSA:168516 |
| Debian -- Security Information -- DSA-821-1 python2.3 | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-821 |
| TSLSA-2005-0059 - multi | web.archive.org<br>text/html<br>Inactive Link Not Archived | TRUSTIX TSLSA-2005-0059 |
| Debian -- Security Information -- DSA-819-1 python2.1 | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-819 |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/ |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/ |
| VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 22875 |
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL oval:org.mitre.oval:def:735 |
| | support.avaya.com<br>application/pdf | CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-216.pdf |
| Gentoo Linux Documentation -- libpcre: Heap integer overflow | www.gentoo.org<br>text/html | GENTOO GLSA-200508-17 |
| HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 22691 |
| '[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC | marc.info<br>text/html | HP SSRT090208 |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20210330 svn commit: r1073139 [3/13] - in /websites/staging/httpd/trunk/content: ./ security/json/ |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [httpd-cvs] 20190815 svn commit: r1048743 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| Secunia - Advisories - SCO OpenServer Updates for Multiple Packages | web.archive.org<br>text/html | SECUNIA 19193 |
| Security Announcement | web.archive.org<br>text/html<br>Inactive Link Not Archived | SUSE SUSE-SA:2005:048 |
| Webmail - OVH | www.vupen.com<br>text/html | VUPEN ADV-2005-2659 |
| No Description Provided | patches.sgi.com | SGI 20060401-01-U |

| | | |
|---|---|---|
| | Inactive Link Not Archived | |
| rhn.redhat.com \| Red Hat Support | www.redhat.com text/html | REDHAT RHSA-2005:761 |
| '[OpenPKG-SA-2005.018] OpenPKG Security Advisory (pcre)' - MARC | marc.info text/html | OPENPKG OpenPKG-SA-2005.018 |
| Ethereal: enpa-sa-00021 | www.ethereal.com text/xml | CONFIRM www.ethereal.com/appnotes/enpa-sa-00021.html |
| Security Announcement | web.archive.org text/html Inactive Link Not Archived | SUSE SUSE-SA:2005:049 |
| Webmail - OVH | www.vupen.com text/html | VUPEN ADV-2006-4502 |
| #102198: Security Vulnerabilities in the Apache 2 Web Server | web.archive.org text/html Inactive Link Not Archived | SUNALERT 102198 |
| Pony Mail! | lists.apache.org text/html | MLIST [httpd-cvs] 20210606 svn commit: r1075470 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2020-13938.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| Gentoo Linux Documentation -- Apache, mod_ssl: Multiple vulnerabilities | www.gentoo.org text/html | GENTOO GLSA-200509-12 |
| PHP: PHP 4.4.1 Release Announcement | www.php.net text/html | CONFIRM www.php.net/release_4_4_1.php |
| ASA-2006-159 (RHSA-2006-0197) | support.avaya.com text/html | CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-159.htm |
| Gentoo Linux Documentation -- Python: Heap overflow in the included PCRE library | www.gentoo.org text/html | GENTOO GLSA-200509-08 |
| | support.avaya.com application/pdf | CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-223.pdf |
| Repository / Oval Repository | oval.cisecurity.org text/html | OVAL oval:org.mitre.oval:def:1496 |
| Security Announcement | web.archive.org text/html Inactive Link Not Archived | SUSE SUSE-SA:2005:052 |
| SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia | web.archive.org text/html | SECUNIA 19532 |
| Pony Mail! | lists.apache.org text/html | MLIST [httpd-cvs] 20210330 svn commit: r1073149 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/ |
| Gentoo Linux Documentation -- PHP: Vulnerabilities in included PCRE and XML-RPC libraries | www.gentoo.org text/html | GENTOO GLSA-200509-19 |
| RETIRED: Apple Mac OS X Security Update 2005-009 Multiple Vulnerabilities | cve.report (archive) text/html | BID 15647 |
| 'SUSE Security Announcement: php4, | marc.info | SUSE SUSE-SA:2005:051 |

| | | |
|---|---|---|
| php5 remote code execution - MARC | text/html | |
| SecurityReason | securityreason.com<br>text/html | SREASON 604 |
| Debian -- Security Information -- DSA-800-1 pcre3 | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-800 |
| Secunia - Advisories - Avaya Intuity LX Two Vulnerabilities | web.archive.org<br>text/html | SECUNIA 17252 |
| Secunia - Advisories - Debian update for pcre3 | web.archive.org<br>text/html | SECUNIA 16679 |
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL oval:org.mitre.oval:def:11516 |
| SecurityTracker.com Archives - PCRE Heap Overflow May Let Users Execute Arbitrary Code | Patch<br>securitytracker.com<br>text/html | SECTRACK 1014744 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Pcre | Pcre | 5.0 | All | All | All |
| Application | Pcre | Pcre | 6.0 | All | All | All |
| Application | Pcre | Pcre | 6.1 | All | All | All |
| Application | Pcre | Pcre | 5.0 | All | All | All |
| Application | Pcre | Pcre | 6.0 | All | All | All |
| Application | Pcre | Pcre | 6.1 | All | All | All |

cpe:2.3:a:pcre:pcre:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:pcre:pcre:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:pcre:pcre:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:pcre:pcre:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:pcre:pcre:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:pcre:pcre:6.1:*:*:*:*:*:*:*:

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**