



# CVE-2005-1268

Published on: 08/05/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:15:00 AM UTC

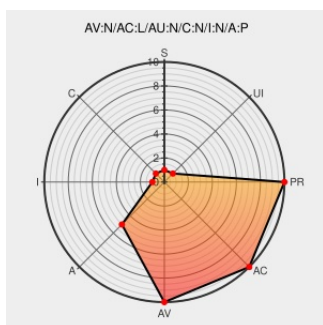
## CVE-2005-1268

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

Off-by-one error in the mod\_ssl Certificate Revocation List (CRL) verification callback in Apache, when configured to use a CRL, allows remote attackers to cause a denial of service (child process crash) via a CRL that causes a buffer overflow of one null byte.

CVE-2005-1268 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**NONE**

Integrity  
Impact

**NONE**

Availability  
Impact

**PARTIAL**

## CVE References

Description

Tags

Link

Pony Mail!

[lists.apache.org](#)  
[text/html](#)

MLIST [httpd-cvs] 20210330 svn commit: r1073149 [4/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/

Advisories - Mandriva

[Broken Link](#)  
[Third Party Advisory](#)  
[www.mandriva.com](#)  
[text/html](#)

MANDRAKE MDKSA-2005:129

Secunia - Advisories -  
Sun Solaris Multiple  
Apache2 Vulnerabilities

[Third Party Advisory](#)  
[web.archive.org](#)  
[text/html](#)

SECUNIA 19072

Security Announcement

[Broken Link](#)  
[web.archive.org](#)  
[text/html](#)  
[Inactive Link](#) [Not Archived](#)

SUSE SUSE-SA:2005:046

|                                                                        |                                                                                                                                                                       |                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SecurityFocus                                                          | <a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="http://www.securityfocus.com">www.securityfocus.com</a><br><a href="#">text/html</a>    | HP SSRT051251                                                                                                                                                                                                                                                               |
| Pony Mail!                                                             | <a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                                                                                   | MLIST [httpd-cvs] 20210330 svn commit: r1888194 [3/13] - /httpd/site/trunk/content/security/json/                                                                                                                                                                           |
| Pony Mail!                                                             | <a href="#">Mailing List</a><br><a href="#">Vendor Advisory</a><br><a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                | 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       | <a href="#">Third Party Advisory</a><br><a href="http://www.vupen.com">www.vupen.com</a><br><a href="#">inode/x-empty</a>                                             | VUPEN ADV-2006-0789                                                                                                                                                                                                                                                         |
| Pony Mail!                                                             | <a href="#">Mailing List</a><br><a href="#">Vendor Advisory</a><br><a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                | 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:                                                           | <a href="#">Third Party Advisory</a><br><a href="http://support.avaya.com">support.avaya.com</a><br><a href="#">text/html</a>                                         | CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-081.htm                                                                                                                                                                                                               |
| Pony Mail!                                                             | <a href="#">Mailing List</a><br><a href="#">Vendor Advisory</a><br><a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                | 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!                                                             | <a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                                                                                   | 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          |
| TLSA-2005-0059 - multi                                                 | <a href="#">Broken Link</a><br><a href="http://web.archive.org">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <b>Not Archived</b> | TRUSTIX TLSA-2005-0059                                                                                                                                                                                                                                                      |
| Secunia - Advisories - SmoothWall Express Update for Multiple Packages | <a href="#">Third Party Advisory</a><br><a href="http://web.archive.org">web.archive.org</a><br><a href="#">text/html</a>                                             | SECUNIA 19185                                                                                                                                                                                                                                                               |
| Pony Mail!                                                             | <a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                                                                                   | MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/                                                                                                                                                        |
| Pony Mail!                                                             | <a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                                                                                   | MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/                                                                                                                                                              |
| Apache mod_ssl CRL Handling Off-By-One Buffer Overflow Vulnerability   | <a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">cve.report (archive)</a><br><a href="#">text/html</a>                                | BID 14366                                                                                                                                                                                                                                                                   |
| Pony Mail!                                                             | <a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                                                                                   | MLIST [httpd-cvs] 20210330 svn commit: r1073139 [3/13] - in /websites/staging/httpd/trunk/content: ./ security/json/                                                                                                                                                        |
| Pony Mail!                                                             | <a href="http://lists.apache.org">lists.apache.org</a><br><a href="#">text/html</a>                                                                                   | 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 |
| Repository / Oval Repository                                           | <a href="#">Third Party Advisory</a>                                                                                                                                  | OVAL oval:org.mitre.oval:def:1346                                                                                                                                                                                                                                           |

|                                                              |                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Repository                                                   | <a href="#">oval.cisecurity.org</a><br><a href="#">text/html</a>                                                                                            |                                                                                                                                                                                                                                                                                                                                                              |
| rhn.redhat.com   Red Hat Support                             | <a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a><br>Inactive Link Not Archived |  REDHAT RHSA-2005:582                                                                                                                                                                                                                                                       |
| 163013 – CAN-2005-1268 mod_ssl off-by-one                    | <a href="#">Issue Tracking</a><br><a href="#">Third Party Advisory</a><br><a href="#">bugzilla.redhat.com</a><br><a href="#">text/html</a>                  |  MISC bugzilla.redhat.com/bugzilla/show_bug.cgi?id=163013                                                                                                                                                                                                                   |
| Repository / Oval Repository                                 | <a href="#">Third Party Advisory</a><br><a href="#">oval.cisecurity.org</a><br><a href="#">text/html</a>                                                    |  OVAL oval:org.mitre.oval:def:9589                                                                                                                                                                                                                                          |
| #102198: Security Vulnerabilities in the Apache 2 Web Server | Broken Link<br><a href="#">web.archive.org</a><br><a href="#">text/html</a><br>Inactive Link Not Archived                                                   |  SUNALERT 102198                                                                                                                                                                                                                                                            |
| Pony Mail!                                                   | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                               |  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 |
| Repository / Oval Repository                                 | <a href="#">Third Party Advisory</a><br><a href="#">oval.cisecurity.org</a><br><a href="#">text/html</a>                                                    |  OVAL oval:org.mitre.oval:def:1714                                                                                                                                                                                                                                          |
| Repository / Oval Repository                                 | <a href="#">Third Party Advisory</a><br><a href="#">oval.cisecurity.org</a><br><a href="#">text/html</a>                                                    |  OVAL oval:org.mitre.oval:def:1747                                                                                                                                                                                                                                        |
| Security Announcement                                        | Broken Link<br><a href="#">web.archive.org</a><br><a href="#">text/html</a><br>Inactive Link Not Archived                                                   |  SUSE SUSE-SR:2005:018                                                                                                                                                                                                                                                    |
| Pony Mail!                                                   | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                               |  MLIST [httpd-cvs] 20210330 svn commit: r1073149 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/                                                                                                                                           |
| Debian -- Security Information -- DSA-805-1 apache2          | <a href="#">Third Party Advisory</a><br><a href="#">www.debian.org</a><br>Deprecated Link<br><a href="#">text/html</a>                                      |  DEBIAN DSA-805                                                                                                                                                                                                                                                           |
| SecurityReason                                               | <a href="#">Third Party Advisory</a><br><a href="#">securityreason.com</a><br><a href="#">text/html</a>                                                     |  SREASON 604                                                                                                                                                                                                                                                              |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------|--------|---------|---------|--------|---------|----------|
|------|--------|---------|---------|--------|---------|----------|

|                                                      |        |                              |     |     |     |     |
|------------------------------------------------------|--------|------------------------------|-----|-----|-----|-----|
| Application                                          | Apache | Http Server                  | All | All | All | All |
| Operating System                                     | Debian | Debian Linux                 | 3.1 | All | All | All |
| Operating System                                     | Debian | Debian Linux                 | 3.1 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Desktop     | 3.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Desktop     | 4.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Desktop     | 3.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Desktop     | 4.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Server      | 3.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Server      | 4.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Server      | 3.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Server      | 4.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Workstation | 3.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Workstation | 4.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Workstation | 3.0 | All | All | All |
| Operating System                                     | Redhat | Enterprise Linux Workstation | 4.0 | All | All | All |
| cpe:2.3:a:apache:http_server:*****:                  |        |                              |     |     |     |     |
| cpe:2.3:o:debian:debian_linux:3.1:*****:             |        |                              |     |     |     |     |
| cpe:2.3:o:debian:debian_linux:3.1:*****:             |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:3.0:*****: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:4.0:*****: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:3.0:*****: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:4.0:*****: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server:3.0:*****:  |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server:4.0:*****:  |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server:3.0:*****:  |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server:4.0:*****:  |        |                              |     |     |     |     |

|                                                              |
|--------------------------------------------------------------|
| cpe:2.3:o:redhat:enterprise_linux_server:4.0.*:*:*:*:*:      |
| cpe:2.3:o:redhat:enterprise_linux_workstation:3.0.*:*:*:*:*: |
| cpe:2.3:o:redhat:enterprise_linux_workstation:4.0.*:*:*:*:*: |
| cpe:2.3:o:redhat:enterprise_linux_workstation:3.0.*:*:*:*:*: |
| cpe:2.3:o:redhat:enterprise_linux_workstation:4.0.*:*:*:*:*: |

## Social Mentions

| Source                                                                                     | Title                                                                           | Posted (UTC)           |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|------------------------|
|  /r/debian | <a href="#">Help with checking changelog history on installed applications.</a> | 2016-12-14<br>09:17:33 |

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)