



CVE-2005-2728

Published on: 08/29/2005 12:00:00 AM UTC

Last Modified on: 06/06/2021 11:15:00 AM UTC

CVE-2005-2728

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The byte-range filter in Apache 2.0 before 2.0.54 allows remote attackers to cause a denial of service (memory consumption) via an HTTP header with a large Range field.

CVE-2005-2728 has been assigned by [M](#) cve@mitre.org 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

Secunia - Advisories - IBM HTTP Server PCRE and Byte-Range Filter Vulnerabilities

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

[X SECUNIA 17036](#)

Pony Mail!

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

[MLIST \[httpd-cvs\] 20210330 svn commit: r1073139 \[4/13\] - in /websites/staging/httpd/trunk/content: ./ security/json/](#)

Secunia - Advisories - Sun Solaris Multiple Apache2 Vulnerabilities

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

[X SECUNIA 19072](#)

Gentoo Linux Documentation -- Apache 2.0: Denial of Service vulnerability

[Patch](#)
[Vendor Advisory](#)
[www.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-200508-15](#)

Secunia - Advisories - Mandriva

[web.archive.org](#)

[X SECUNIA 16753](#)

update for apache2	text/html	
SecurityFocus	www.securityfocus.com text/html	 HP SSRT051251
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com inode/x-empty	 VUPEN ADV-2006-0789
1. Overview:	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-081.htm
Pony Mail!	lists.apache.org 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
Secunia - Advisories - Mandriva update for apache2	web.archive.org text/html	 SECUNIA 18161
usn/usn-177-1 - Ubuntu Linux	www.ubuntu.com text/html	 UBUNTU USN-177-1
TLSA-2005-0059 - multi	web.archive.org text/html Inactive Link Not Archived	 TRUSTIX TLSA-2005-0059
Secunia - Advisories - Ubuntu update for apache2	web.archive.org text/html	 SECUNIA 17923
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10017
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20060101-01-U
Secunia - Advisories - Ubuntu Updates for Multiple Packages	web.archive.org text/html	 SECUNIA 16714
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2005:051
Secunia - Advisories - Trustix update for multiple packages	web.archive.org text/html	 SECUNIA 16789
Pony Mail!	lists.apache.org 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 - SGI Advanced Linux Environment Multiple Updates	web.archive.org text/html	 SECUNIA 18517
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:608
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	web.archive.org text/html	 SECUNIA 16743
Secunia - Advisories - Fedora update for httpd	web.archive.org text/html	 SECUNIA 16746

Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1727
Secunia - Advisories - Trustix update for multiple packages	web.archive.org text/html	 SECUNIA 17288
Secunia - Advisories - Apache Byte-Range Filter and MPM Worker Denial of Service Vulnerabilities	Vendor Advisory web.archive.org text/html	 SECUNIA 16559
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	 SECUNIA 17831
Secunia - Advisories - Red Hat update for httpd/mod_ssl	web.archive.org text/html	 SECUNIA 16705
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
#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
Advisories - Mandriva	www.mandriva.com text/html	 MANDRIVA MDKSA-2005:161
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2005:052
Secunia - Advisories - Red Hat update for httpd	web.archive.org text/html	 SECUNIA 18333
Secunia - Advisories - Debian update for apache2	web.archive.org text/html	 SECUNIA 16754
Apache CGI Byterange Request Denial of Service Vulnerability	Patch cve.report (archive) text/html	 BID 14660
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1246
Pony Mail!	lists.apache.org 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
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/
Secunia - Advisories - SUSE update for apache2	web.archive.org text/html	 SECUNIA 16769
Debian -- Security Information -- DSA-805-1 apache2	www.debian.org Deprecated Link text/html	 DEBIAN DSA-805
Pony Mail!	lists.apache.org 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](#)

SecurityReason

[securityreason.com](#)
[text/html](#)

 SREASON 604

Secunia - Advisories - Avaya
Products httpd/mod_ssl
Vulnerabilities

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

 SECUNIA 16956

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

 OVAL oval.org.mitre.oval:def:760

Pony Mail!

[lists.apache.org](#)
[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

Pony Mail!

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

 MLIST [httpd-cvs] 20210330 svn commit: r1073149 [5/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/

29962 – byterange filter buffers
response in memory

[Patch](#)
[Vendor Advisory](#)
[issues.apache.org](#)
[text/html](#)

 CONFIRM issues.apache.org/bugzilla/show_bug.cgi?id=29962

Secunia - Advisories - HP-UX
Apache Multiple Vulnerabilities

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

 SECUNIA 17600

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

 XF apache-byterange-dos(22006)

Pony Mail!

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

 MLIST [httpd-cvs] 20210330 svn commit: r1888194 [4/13] - /httpd/site/trunk/content/security/json/

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.

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	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All

Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All

Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All
cpe:2.3:a:apache:http_server:2.0:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.28:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.28:beta:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.32:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.35:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.36:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.37:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.38:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.39:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.40:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.41:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.42:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.43:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.44:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.45:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.46:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.47:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.48:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.49:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.50:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.51:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.52:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.53:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.9:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:2.0.28:*:*:*:*:*:						

cpe:2.3:a:apache:http_server:2.0.28:beta:*****:
cpe:2.3:a:apache:http_server:2.0.32:*****:
cpe:2.3:a:apache:http_server:2.0.35:*****:
cpe:2.3:a:apache:http_server:2.0.36:*****:
cpe:2.3:a:apache:http_server:2.0.37:*****:
cpe:2.3:a:apache:http_server:2.0.38:*****:
cpe:2.3:a:apache:http_server:2.0.39:*****:
cpe:2.3:a:apache:http_server:2.0.40:*****:
cpe:2.3:a:apache:http_server:2.0.41:*****:
cpe:2.3:a:apache:http_server:2.0.42:*****:
cpe:2.3:a:apache:http_server:2.0.43:*****:
cpe:2.3:a:apache:http_server:2.0.44:*****:
cpe:2.3:a:apache:http_server:2.0.45:*****:
cpe:2.3:a:apache:http_server:2.0.46:*****:
cpe:2.3:a:apache:http_server:2.0.47:*****:
cpe:2.3:a:apache:http_server:2.0.48:*****:
cpe:2.3:a:apache:http_server:2.0.49:*****:
cpe:2.3:a:apache:http_server:2.0.50:*****:
cpe:2.3:a:apache:http_server:2.0.51:*****:
cpe:2.3:a:apache:http_server:2.0.52:*****:
cpe:2.3:a:apache:http_server:2.0.53:*****:
cpe:2.3:a:apache:http_server:2.0.9:*****:

Social Mentions		
Source	Title	Posted (UTC)
 /r/debian	Help with checking changelog history on installed applications.	2016-12-14 09:17:33
← Previous ID		Next ID →

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](#)