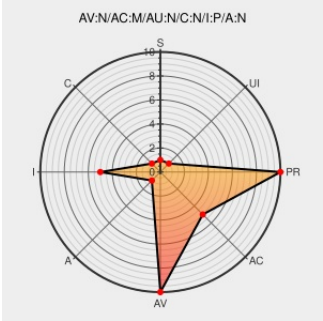
CVE-2005-2088

Published on: 06/30/2005 12:00:00 AM UTC

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

CVE-2005-2088

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



Certain versions of Http Server from Apache contain the following vulnerability:

The Apache HTTP server before 1.3.34, and 2.0.x before 2.0.55, when acting as an HTTP proxy, allows remote attackers to poison the web cache, bypass web application firewall protection, and conduct XSS attacks via an HTTP request with both a "Transfer-Encoding: chunked" header and a Content-Length header, which causes Apache to incorrectly handle and forward the body of the request in a way that causes the receiving server to process it as a separate HTTP request, aka "HTTP Request Smuggling."

CVE-2005-2088 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
usn/usn-160-2 - Ubuntu Linux	web.archive.org text/html Inactive Link Not Archived	UBUNTU USN-160-2
Secunia - Advisories - Slackware update for apache/mod_ssl	web.archive.org text/html	SECUNIA 17487
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-1018
Advisories - Mandriva Linux	www.mandriva.com	MANDRIVA MDKSA-2005:130

	text/html	
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/
About Security Update 2005-009	web.archive.org text/html Inactive Link Not Archived	APPLE APPLE-SA-2005-11-29
No Description Provided	secure-support.novell.com Inactive Link Not Archived	CONFIRM secure-support.novell.com/KanisaPlatform/Publishing/741/3222109_f.SAL_Public.html
Debian -- Security Information -- DSA-803-1 apache	www.debian.org Depreciated Link text/html	DEBIAN DSA-803
Secunia - Advisories - Mac OS X Security Update Fixes Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 17813
Secunia - Advisories - HP VirtualVault Apache HTTP Request Smuggling Vulnerability	web.archive.org text/html	SECUNIA 19317
IBM Software | IBM	www.watchfire.com application/pdf	MISC www.watchfire.com/resources/HTTP-Request-Smuggling.pdf
Secunia - Advisories - Sun Solaris Multiple Apache2 Vulnerabilities	web.archive.org text/html	SECUNIA 19072
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2005:046
404 Not Found	www.apache.org text/plain Inactive Link Not Archived	CONFIRM www.apache.org/dist/httpd/CHANGES_1.3
SecurityFocus	www.securityfocus.com text/html	HP SSRT051251
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1888194 [3/13] - /httpd/site/trunk/content/security/json/
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
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com inode/x-empty	VUPEN ADV-2006-0789
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
1. Overview:	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-081.htm
Secunia - Advisories - Apache HTTP Request Smuggling Vulnerability	web.archive.org text/html	SECUNIA 14530

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
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 - Sun Solaris Multiple Apache Vulnerabilities	web.archive.org text/html	SECUNIA 19073
TSLSA-2005-0059 - multi	web.archive.org text/html Inactive Link Not Archived	TRUSTIX TSLSA-2005-0059
SecurityTracker.com Archives - Apache Chunked Transfer-Encoding and Content-Length Processing Lets Remote Users Smuggle HTTP Requests	securitytracker.com text/html	SECTRACK 1014323
Secunia - Advisories - SmoothWall Express Update for Multiple Packages	web.archive.org text/html	SECUNIA 19185
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
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:840
No Description Provided	www1.itrc.hp.com Inactive Link Not Archived	HP HPSBUX02101
Support	www.redhat.com text/html	REDHAT RHSA-2005:582
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [3/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
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
with a space causes the title to be misaligned in the listing. [David J. MacKenzie] *) Change mod_cern_meta to be configurable on a per-directory basis. [David J. MacKenzie] *) Add 'Include' directive to allow inclusion of configuration files within configuration files. [Randy Terbush] *) Proxy errors on connect() are logged to the error_log (nothing new); now they include the IP address and port that failed (*that's*	www.apache.org text/plain Inactive Link Not Archived	CONFIRM www.apache.org/dist/httpd/CHANGES_2.0

and port that failed (that's new). [Ken Coar, Marc Slemko] PR#352 *) Various ar		
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2659
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11452
Bugtraq: A new whitepaper by Watchfire - HTTP Request Smuggling	seclists.org text/html	BUGTRAQ 20050606 A new whitepaper by Watchfire - HTTP Request Smuggling
Novell NetWare Apache HTTP Request Smuggling Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 23074
SecuriTeam.com ™ - HTTP Request Smuggling	Exploit www.securiteam.com text/html	MISC www.securiteam.com/securityreviews/5GP0220G0U.html
The Slackware Linux Project: Slackware Security Advisories	slackware.com text/html	SLACKWARE SSA:2005-310-04
Secunia - Advisories - IBM HTTP Server HTTP Request Smuggling and mod_imap Vulnerabilities	web.archive.org text/html	SECUNIA 17319
IBM Search results - United States	www-1.ibm.com text/html	AIXAPAR PK13959
#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
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1526
Apache HTTP Request Smuggling Vulnerability	cve.report (archive) text/html	BID 14106
'[Announce] Apache HTTP Server 2.0.55 Released' - MARC	marc.info text/html	MLIST [apache-httpd-announce] 20051014 Apache HTTP Server 2.0.55 Released
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1629
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1237
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-4680
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2140
Search results	www-1.ibm.com text/html	AIXAPAR PK16139
Security Announcement	web.archive.org	SUSE SUSE-SR:2005:018

	text/html Inactive Link Not Archived	
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/
Debian -- Security Information -- DSA-805-1 apache2	www.debian.org Depreciated Link text/html	DEBIAN DSA-805
RETIRED: Apple Mac OS X Security Update 2005-009 Multiple Vulnerabilities	cve.report (archive) text/html	BID 15647
SecurityReason	securityreason.com text/html	SREASON 604
#102197: Security Vulnerabilities in the Apache 1.3 Web Server	web.archive.org text/html Inactive Link Not Archived	SUNALERT 102197

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	1.3.29	All	All	All
Application	Apache	Http Server	1.3.30	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.32	All	All	All
Application	Apache	Http Server	1.3.33	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	2.0.54	All	All	All
Application	Apache	Http Server	1.3.29	All	All	All
Application	Apache	Http Server	1.3.30	All	All	All

Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.32	All	All	All
Application	Apache	Http Server	1.3.33	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	2.0.54	All	All	All
Application	Apache	Http Server	All	All	All	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All

cpe:2.3:a:apache:http_server:1.3.29:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.30:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.31:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.32:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.33:*:*:*:*:*:*:*:

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:2.0.54:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.54:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.29:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.30:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.31:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.32:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.33:*:*:*:*:*:*:*:

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:2.0.54:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:*:*:*:*:*:*:

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→

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