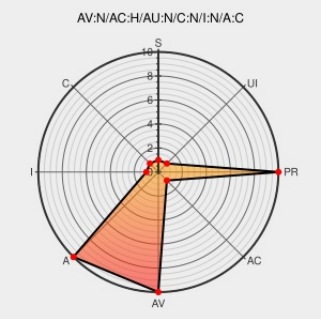
CVE-2005-3357

Published on: 12/31/2005 05:00:00 AM UTC

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

CVE-2005-3357

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



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

mod_ssl in Apache 2.0 up to 2.0.55, when configured with an SSL vhost with access control and a custom error 400 error page, allows remote attackers to cause a denial of service (application crash) via a non-SSL request to an SSL port, which triggers a NULL pointer dereference.

CVE-2005-3357 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	FEDORA FLSA-2006:175406
	Patch Vendor Advisory www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX TSLSA-2005-0074
SecurityFocus	www.securityfocus.com text/html	HP HPSBUX02145
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 - Trustix update for apache	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18340
#102640: Security Vulnerability in Apache 2 Web Server Module 'mod_ssl'	web.archive.org text/html Inactive Link Not Archived	SUNALERT 102640
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-4300
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210603 svn commit: r1075360 [1/3] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
HP-UX update for Apache - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 23260
HPSBMA02328 SSRT071293 rev.2 - HP OpenView Network Node Manager (OV NNM) Running Apache, Remote Cross Site Scripting (XSS), Denial of Service (DoS), Execute Arbitrary Code - c01428449 - HP Business Support Center	web.archive.org text/html Inactive Link Not Archived	HP SSRT071293
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 - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2008-1246
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
Gentoo Linux Documentation -- Apache: Multiple vulnerabilities	Patch Vendor Advisory www.gentoo.org text/html	GENTOO GLSA-200602-03
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/
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
Sun Solaris update for Apache 2 mod_ssl module - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22233
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073140 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/cveisontohtml.py security/vulnerabilities_13.html

		security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Secunia - Advisories - Fedora update for httpd	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18585
USN-241-1: Apache vulnerabilities | Ubuntu security notices | Ubuntu	www.ubuntulinux.org text/html	UBUNTU USN-241-1
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210606 svn commit: r1075470 [3/4] - 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
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2008-1697
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210606 svn commit: r1075467 [2/2] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Secunia - Advisories - Apache 2 mod_ssl Denial of Service Vulnerability	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18307
No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20060101-01-U
Secunia - Advisories - Ubuntu update for apache/apache2	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18429
rhn.redhat.com | Red Hat Support	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2006:0159
HP OpenView Network Node Manager Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 29849
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-4207
'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC	marc.info text/html	HP SSRT090208
Apache Mod_SSL Custom Error Document Remote Denial Of Service Vulnerability	cve.report (archive) text/html	BID 16152

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 - Gentoo update for apache	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18743
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-4868
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18517
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-3995
Avaya CMS Sun Solaris X Display Manager Security Issue - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22992
IBM - Subscription service - Bulletin	web.archive.org text/html Inactive Link Not Archived	CONFIRM www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117
#102662: Security Vulnerabilities in the Apache 2.0 Web Server "mod_rewrite" Module	web.archive.org text/html Inactive Link Not Archived	SUNALERT 102662
HP-UX VirtualVault / Webproxy Apache Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22669
SecurityFocus	www.securityfocus.com text/html	HP SSRT061269
[SECURITY] Fedora Core 4 Update: httpd-2.0.54-10.3	Patch www.redhat.com text/html	FEDORA FEDORA-2006-052
Bug 37791 – SEGV if the client is connection plain to a SSL enabled port	issues.apache.org text/html	CONFIRM issues.apache.org/bugzilla/show_bug.cgi?id=37791
US-CERT Technical Cyber Security Alert TA08-150A -- Apple Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/html	CERT TA08-150A
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-3920
Sun Solaris update for Apache 2 - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22368
[Apache-SVN] Revision 358026	svn.apache.org text/html	MISC svn.apache.org/viewcvs?rev=358026&view=rev
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11467
Pony Mail!		MLIST [httpd-cvs] 20210602 svn commit: r1075260 [2/2]

Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210603 svn commit: r1075360 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json 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] 20210606 svn commit: r1075467 [1/2] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
SUSE Updates for Multiple Packages - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 19012
SUSE Security Announcement: Apache2 security problems (SUSE-SA:2006:051)	lists.opensuse.org text/html	SUSE SuSE-SA:2006:051
Secunia - Advisories - Red Hat update for httpd	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18333
SecurityTracker.com Archives - Apache mod_ssl Null Pointer Dereference May Let Remote Users Deny Service	securitytracker.com text/html	SECTRACK 1015447
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 30430
IBM HMC Apache2 / OpenSSL Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22523
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-0056
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/
SUSE update for apache2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 21848
ASA-2006-250 (SUN 102606, 102636, 102640, 102648, 102651, 102652, 102655, 102657)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-250.htm
APPLE-SA-2008-05-28 Security Update 2008-003 and Mac OS X v10.5.3	lists.apple.com text/html	APPLE APPLE-SA-2008-05-28
SuSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:004	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2006:004
Secunia - Advisories - Mandriva update for apache2	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18339
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1888194 [4/13] - /httpd/site/trunk/content/security/json/

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

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	2.0.54	All	All	All
Application	Apache	Http Server	2.0.55	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	2.0.54	All	All	All
Application	Apache	Http Server	2.0.55	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:2.0.54:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.55:*:*:*:*:*:*:*:

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

cpe:2.3:a:apache:http_server:2.0.55:*:*:*:*:*:*:*

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→