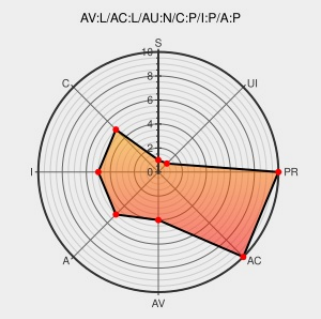
CVE-2004-0747

Published on: 09/17/2004 12:00:00 AM UTC

Last Modified on: 11/07/2023 01:56:00 AM UTC

CVE-2004-0747

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



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

Buffer overflow in Apache 2.0.50 and earlier allows local users to gain apache privileges via a .htaccess file that causes the overflow during expansion of environment variables.

CVE-2004-0747 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CA ARCserve Backup Apache HTTP Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 34920
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2004:032
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./security/json/
Secunia - Advisories - Apache apr-util Library and Environment Variable Expansion Vulnerabilities	web.archive.org text/html	SECUNIA 12540
Pony Mail!	lists.apache.org	MLIST [httpd-cvs] 20210422 svn commit: r1074079 [2/3]

	text/html	- in /websites/staging/httpd/trunk/content: ./ apreq/ contribute/ contributors/ dev/ docs-project/ docs/ info/ mod_fcgid/ mod_ftp/ mod_mbox/ mod_smtpd/ modules/ security/ test/ test/flood/
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
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] 20210330 svn commit: r1888194 [3/13] - /httpd/site/trunk/content/security/json/
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
SecurityTracker.com Archives - Apache ap_resolve_env() Buffer Overflow in Reading Configuration Files May Let Local Users Gain Elevated Privileges	securitytracker.com text/html	SECTRACK 1011303
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/
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
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
No Description Provided	www.mandrakesecure.net Inactive Link Not Archived	MANDRAKE MDKSA-2004:096
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [3/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
US-CERT Vulnerability Note VU#481998	US Government Resource www.kb.cert.org text/html	CERT-VN VU#481998
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
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11561
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2009-1233
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/
redhat.com | Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2004:463
	www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX 2004-0047
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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF apache-env-configuration-bo(17384)
Gentoo Linux Documentation -- Apache 2, mod_dav: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200409-21
404 Not Found	support.ca.com text/html Inactive Link Not Archived	MISC support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=205147

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
Application	Apache	Http Server	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.32	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	All	All	All
Application	Apache	Http Server	2.0.28	All	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

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

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:2.0.32:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.28:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*

← Previous ID

Next ID→