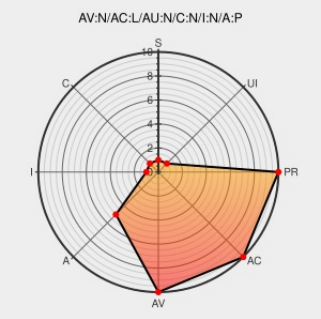
CVE-2002-1593

Published on: 09/25/2002 04:00:00 AM UTC

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

CVE-2002-1593

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



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

mod_dav in Apache before 2.0.42 does not properly handle versioning hooks, which may allow remote attackers to kill a child process via a null dereference and cause a denial of service (CPU consumption) in a preforked multi-processing module.

CVE-2002-1593 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Apache 2 mod_dav Denial Of Service Vulnerability	Patch, cve.report (archive), text/html	BID 5816
Apache Web Server 'mod_dav' Has Null Pointer Bug That May Allow Remote Users to Cause Denial of Service Conditions - SecurityTracker	securitytracker.com, text/html	SECTRACK 1005285
Pony Mail!	lists.apache.org, text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073139 [2/13] - in /websites/staging/httpd/trunk/content: ./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/cveisontohtml.py

		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-mod-dav-dos(10208)
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] 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* new). [Ken Coar, Marc Slemko] PR#352 *) Various ar	www.apache.org text/plain Inactive Link Not Archived	CONFIRM www.apache.org/dist/httpd/CHANGES_2.0
CERT/CC Vulnerability Note VU#406121	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#406121
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1888194 [2/13] - /httpd/site/trunk/content/security/json/
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] 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
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210330 svn commit: r1073149 [2/13] - in /websites/staging/httpd/trunk/content: ./ security/ 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

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] 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] 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

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	2.0.32	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	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

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

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

← Previous ID

Next ID→

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