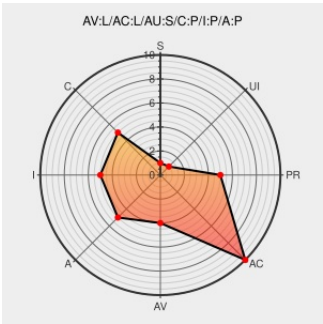
CVE-2003-1307

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1307

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



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

** DISPUTED ** The mod_php module for the Apache HTTP Server allows local users with write access to PHP scripts to send signals to the server's process group and use the server's file descriptors, as demonstrated by sending a STOP signal, then intercepting incoming connections on the server's TCP port. NOTE: the PHP developer has disputed this vulnerability, saying "The opened file descriptors are opened by Apache. It is the job of Apache to protect them ... Not a bug in PHP."

CVE-2003-1307 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	www.securityfocus.com text/x-c	BUGTRAQ 20061020 Re: PHP "exec", "system", "popen" (+small POC)
Apache mod_php Module File Descriptor Leakage Vulnerability	Exploit cve.report (archive) text/html	BID 9302
PHP Bugs: #38915: mod_php: system() (and similar) don't cleanup opened handles of Apache	Exploit bugs.php.net text/html	MISC bugs.php.net/38915
Page not found · GitHub Pages	Exploit	MISC hackerdom.ru/~dimmo/phpexpl.c

	hackerdom.ru text/x-c Inactive Link Not Archived	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061019 PHP "exec", "system", "popen" problem
SecurityFocus HOME Mailing List: BugTraq	Exploit Vendor Advisory www.securityfocus.com text/html	BUGTRAQ 20031226 Hijacking Apache https by mod_php

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	2.0.28	beta	win32	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.32	beta	win32	All
Application	Apache	Http Server	2.0.34	beta	win32	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	2.0.46	All	win32	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	2.0.9	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	2.0.28	beta	win32	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.32	beta	win32	All
Application	Apache	Http Server	2.0.34	beta	win32	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	2.0.46	All	win32	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	2.0.9	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:2.0.28:beta:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.32:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.32:beta:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.34:beta:win32:*:*:*:*:*:

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:2.0.46:*:win32:*:*:*:*:*:

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:2.0.9:*:*:*:*:*:*:*:

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:2.0.28:beta:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.32:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.32:beta:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:2.0.34:beta:win32:*:*:*:*:*:

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:2.0.46:*:win32:*:*:*:*:*:

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:2.0.9:*:*:*:*:*:*:*:

← Previous ID

Next ID→