



CVE-2003-0134

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2003-0134
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-04-11 04:00:00 UTC
Updated	2023-11-07 01:56:00 UTC
Description	Unknown vulnerability in filestat.c for Apache running on OS2, versions 2.0 through 2.0.45, allows unknown attackers to ca

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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	2.0.42	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	2.0.9	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	2.0.32	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	2.0.9	All	All	All

References						
Reference	Source		Link	Tags		
Pony Mail!			lists.apache.org			
'[ANNOUNCE] Apache 2.0.45 Released' - MARC	BUGTRAQ		marc.info			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			
404 Not Found	CONFIRM		cvs.apache.org	Patch		
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			

Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
20030528 [SECURITY] [ANNOUNCE] Apache 2.0.46 released	BUGTRAQ	marc.info	
Pony Mail!	MLIST	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.0.46: http://httpd.apache.org/security/vulnerabilities_20.html
There are currently no legacy QID mappings associated with this CVE.			

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

Free CVE JSON API cve.report/api

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