CVE-2017-9789

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-9789
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-13 16:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	When under stress, closing many connections, the HTTP/2 handling code in Apache httpd 2.4.26 would sometimes access

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.26	All	All	All
Application	Apache	Http Server	2.4.26	All	All	All

References

Reference
Pony Mail!
Pony Mail!
July 2017 Apache httpd Server Vulnerabilities in Multiple NetApp Products | NetApp Product Security
Pony Mail!
Pony Mail!
Pony Mail!
Document Display | HPE Support Center
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple
Pony Mail!
Apache HTTP Server CVE-2017-9789 Denial of Service Vulnerability
Pony Mail!
Pony Mail!

Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Apache mod_http2 Memory Access Error Lets Remote Users Deny Service - SecurityTracker
Pony Mail!
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Apache: Multiple vulnerabilities (GLSA 201710-32) — Gentoo security
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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