



CVE-2017-3169

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

Summary

CVE	CVE-2017-3169
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-20 01:29:00 UTC
Updated	2023-11-07 02:44:00 UTC
Description	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party mo

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.2.0	All	All	All
Application	Apache	Http Server	2.2.11	All	All	All
Application	Apache	Http Server	2.2.12	All	All	All
Application	Apache	Http Server	2.2.13	All	All	All
Application	Apache	Http Server	2.2.14	All	All	All
Application	Apache	Http Server	2.2.15	All	All	All
Application	Apache	Http Server	2.2.16	All	All	All
Application	Apache	Http Server	2.2.17	All	All	All
Application	Apache	Http Server	2.2.18	All	All	All
Application	Apache	Http Server	2.2.19	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.20	All	All	All
Application	Apache	Http Server	2.2.21	All	All	All
Application	Apache	Http Server	2.2.22	All	All	All
Application	Apache	Http Server	2.2.23	All	All	All
Application	Apache	Http Server	2.2.24	All	All	All
Application	Apache	Http Server	2.2.25	All	All	All

Application	Apache	Http Server	2.2.26	All	All	All
Application	Apache	Http Server	2.2.27	All	All	All
Application	Apache	Http Server	2.2.29	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.30	All	All	All
Application	Apache	Http Server	2.2.31	All	All	All
Application	Apache	Http Server	2.2.32	All	All	All
Application	Apache	Http Server	2.4.1	All	All	All
Application	Apache	Http Server	2.4.10	All	All	All
Application	Apache	Http Server	2.4.12	All	All	All
Application	Apache	Http Server	2.4.16	All	All	All
Application	Apache	Http Server	2.4.17	All	All	All
Application	Apache	Http Server	2.4.18	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.20	All	All	All
Application	Apache	Http Server	2.4.23	All	All	All
Application	Apache	Http Server	2.4.25	All	All	All
Application	Apache	Http Server	2.2.0	All	All	All
Application	Apache	Http Server	2.2.11	All	All	All
Application	Apache	Http Server	2.2.12	All	All	All
Application	Apache	Http Server	2.2.13	All	All	All
Application	Apache	Http Server	2.2.14	All	All	All
Application	Apache	Http Server	2.2.15	All	All	All
Application	Apache	Http Server	2.2.16	All	All	All
Application	Apache	Http Server	2.2.17	All	All	All
Application	Apache	Http Server	2.2.18	All	All	All
Application	Apache	Http Server	2.2.19	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.20	All	All	All
Application	Apache	Http Server	2.2.21	All	All	All
Application	Apache	Http Server	2.2.22	All	All	All
Application	Apache	Http Server	2.2.23	All	All	All
Application	Apache	Http Server	2.2.24	All	All	All
Application	Apache	Http Server	2.2.25	All	All	All
Application	Apache	Http Server	2.2.26	All	All	All

Application	Apache	Http Server	2.2.27	All	All	All
Application	Apache	Http Server	2.2.29	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.30	All	All	All
Application	Apache	Http Server	2.2.31	All	All	All
Application	Apache	Http Server	2.2.32	All	All	All
Application	Apache	Http Server	2.4.1	All	All	All
Application	Apache	Http Server	2.4.10	All	All	All
Application	Apache	Http Server	2.4.12	All	All	All
Application	Apache	Http Server	2.4.16	All	All	All
Application	Apache	Http Server	2.4.17	All	All	All
Application	Apache	Http Server	2.4.18	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.20	All	All	All
Application	Apache	Http Server	2.4.23	All	All	All
Application	Apache	Http Server	2.4.25	All	All	All

References

Reference

Pony Mail!

Debian -- Security Information -- DSA-3896-1 apache2

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Apache Mail Archives

Red Hat Customer Portal

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!

Pony Mail!

Pony Mail!

Pony Mail!

Apache HTTPD Bugs Let Remote Users Deny Service and Bypass Authentication in Certain Cases - SecurityTracker

Pony Mail!

NoMachine - Local privileges vulnerability

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

[R1] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Apache Mail Archives

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

June 2017 Apache HTTP Server Vulnerabilities in NetApp Products | NetApp Product Security

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Apache HTTP Server CVE-2017-3169 Denial of Service Vulnerability

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!	
Pony Mail!	
Apache: Multiple vulnerabilities (GLSA 201710-32) — Gentoo security	
Exploits/CVE-2017-3169 at master · gottburgm/Exploits · GitHub	
Pony Mail!	
Pony Mail!	
Oracle Critical Patch Update - October 2017	
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.	
Legacy QID Mappings	
378141 Virtuozzo Linux Security Update for mod_ssl (VZLSA-2017:2478)	
500011 Alpine Linux Security Update for apache2	
503702 Alpine Linux Security Update for apache2	

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)