CVE-2017-9798

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

Summary

CVE	CVE-2017-9798
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-18 15:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .

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	2.4.0	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	2.4.26	All	All	All
Application	Apache	Http Server	2.4.27	All	All	All
Application	Apache	Http Server	2.4.3	All	All	All
Application	Apache	Http Server	2.4.4	All	All	All
Application	Apache	Http Server	2.4.6	All	All	All
Application	Apache	Http Server	2.4.7	All	All	All

Application	Apache	Http Server	2.4.9	All	All	All
Application	Apache	Http Server	2.4.0	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	2.4.26	All	All	All
Application	Apache	Http Server	2.4.27	All	All	All
Application	Apache	Http Server	2.4.3	All	All	All
Application	Apache	Http Server	2.4.4	All	All	All
Application	Apache	Http Server	2.4.6	All	All	All
Application	Apache	Http Server	2.4.7	All	All	All
Application	Apache	Http Server	2.4.9	All	All	All
Application	Apache	Http Server	All	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference
svn.apache.org/viewvc/httpd/httpd/branches/2.4.x/server/core.c
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

Apache < 2.2.34 / < 2.4.27 - HTTP OPTIONS Memory Leak

Pony Mail!

Pony Mail!

Pony Mail!

Apache HTTP Server CVE-2017-9798 Information Disclosure Vulnerability

Pony Mail!

CVE-2017-9798 Apache HTTP Server Vulnerability in NetApp Products | NetApp Product Security

Pony Mail!

Oracle Critical Patch Update - January 2018

CVE-2017-9798

Red Hat Customer Portal

Pony Mail!

CPU July 2018

Oracle Critical Patch Update - April 2018

Pony Mail!

Pony Mail!

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

Pony Mail!

Pony Mail!

Pony Mail!

Debian -- Security Information -- DSA-3980-1 apache2

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

httpd 2.4 vulnerabilities - The Apache HTTP Server Project

blog.fuzzing-project.org/uploads/apache-2.2-optionsbleed-backport.patch

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

Document Display | HPE Support Center
Oracle Critical Patch Update - January 2019
Red Hat Customer Portal
Red Hat Customer Portal
Oracle PeopleSoft Enterprise PeopleTools Multiple Remote Security Vulnerabilities
Pony Mail!
Red Hat Customer Portal
Red Hat Customer Portal
Apache HTTPD Use-After-Free Memory Error in Processing HTTP OPTIONS Requests Lets Remote Users Obtain Potentially Sensitive Inforr
About the security content of macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan - Apple
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Optionsbleed - HTTP OPTIONS method can leak Apache's server memory | The Fuzzing Project
CPU Oct 2018
Red Hat Customer Portal
Pony Mail!
Apache: Multiple vulnerabilities (GLSA 201710-32) — Gentoo security
Pony Mail!
Pony Mail!
Pony Mail!
core: Disallow Methods' registration at run time (.htaccess), they ma… · apache/httpd@4cc2782 · GitHub
GitHub - hannob/optionsbleed
oss-security - Optionsbleed bug in Apache HTTPD
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Oracle Critical Patch Update Advisory - April 2019
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378145 Virtuozzo Linux Security Update for mod_ssl (VZLSA-2017:2972)
- 500012 Alpine Linux Security Update for apache2
- 503703 Alpine Linux Security Update for apache2