CVE-2016-2161

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-2161
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-27 21:29:00 UTC
Updated	2023-11-07 02:31:00 UTC
Description	In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and ea

Risk And Classification

Problem Types: CWE-20

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	2.4.14	All	All	All
Application	Apache	Http Server	2.4.16	All	All	All
Application	Apache	Http Server	2.4.19	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	2.4.21	All	All	All
Application	Apache	Http Server	2.4.22	All	All	All
Application	Apache	Http Server	2.4.23	All	All	All
Application	Apache	Http Server	2.4.3	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	2.4.8	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	2.4.14	All	All	All
Application	Apache	Http Server	2.4.16	All	All	All
Application	Apache	Http Server	2.4.19	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	2.4.21	All	All	All
Application	Apache	Http Server	2.4.22	All	All	All
Application	Apache	Http Server	2.4.23	All	All	All
Application	Apache	Http Server	2.4.3	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	2.4.8	All	All	All
Application	Apache	Http Server	2.4.9	All	All	All

References

Reference
Pony Mail!
Pony Mail!
Apache HTTP Server CVE-2016-2161 Denial of Service Vulnerability
Red Hat Customer Portal
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple
httpd 2.4 vulnerabilities - The Apache HTTP Server Project
Pony Mail!
Red Hat Customer Portal
Pony Mail!
December 2016 Apache HTTP Server Vulnerabilities in Multiple NetApp Products | NetApp Product Security

Pony Mail!
Debian -- Security Information -- DSA-3796-1 apache2
Pony Mail!
Pony Mail!
Pony Mail!
[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Apache HTTPD Multiple Flaws Let Remote Users Deny Service, Conduct HTTP Response Splitting Attacks, and Access and Modify Session I
Pony Mail!
Pony Mail!
Pony Mail!
Document Display | HPE Support Center
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Apache: Multiple vulnerabilities (GLSA 201701-36) — Gentoo security
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

378182 Virtuozzo Linux Security Update for mod_proxy_html (VZLSA-2017:0906)
710461 Gentoo Linux Apache Multiple Vulnerabilities (GLSA 201701-36)

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