CVE-2019-9517

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-9517
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-13 21:15:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of serv

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	Apache	Traffic Server	All	All	All	All
Application	Apache	Traffic Server	All	All	All	All
Application	Apache	Traffic Server	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Application	Apple	Swiftnio	All	All	All	All
Operating System	Canonical	Ubuntu Linux	All	All	All	All
Operating System	Canonical	Ubuntu Linux	All	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Mcafee	Web Gateway	All	All	All	All
Application	Mcafee	Web Gateway	All	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Oracle	Communications Element Manager	8.0.0	All	All	All
Application	Oracle	Communications Element Manager	8.1.0	All	All	All
Application	Oracle	Communications Element Manager	8.1.1	All	All	All
Application	Oracle	Communications Element Manager	8.2.0	All	All	All
Application	Oracle	Communications Element Manager	8.0.0	All	All	All
Application	Oracle	Communications Element Manager	8.1.0	All	All	All
Application	Oracle	Communications Element Manager	8.1.1	All	All	All
Application	Oracle	Communications Element Manager	8.2.0	All	All	All
Application	Oracle	Graalvm	19.2.0	All	All	All
Application	Oracle	Graalvm	19.2.0	All	All	All
Application	Oracle	Instantis Enterprisetrack	All	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Jboss Core Services	1.0	All	All	All
Application	Redhat	Jboss Core Services	1.0	All	All	All

Application	Redhat	Jboss Enterprise Application Platform	7.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.3.0	All	All	All
Application	Redhat	Openshift Service Mesh	1.0	All	All	All
Application	Redhat	Openshift Service Mesh	1.0	All	All	All
Application	Redhat	Quay	3.0.0	All	All	All
Application	Redhat	Quay	3.0.0	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All
Application	Synology	Diskstation Manager	6.2	All	All	All
Application	Synology	Diskstation Manager	6.2	All	All	All
Application	Synology	Skynas	-	All	All	All
Application	Synology	Skynas	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Operating System	Synology	Vs960hd Firmware	-	All	All	All
Operating System	Synology	Vs960hd Firmware	-	All	All	All

References

Reference
Red Hat Customer Portal
Pony Mail!
myF5
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
[SECURITY] Fedora 29 Update: mod_http2-1.15.3-2.fc29 - package-announce - Fedora Mailing-Lists
Pony Mail!
Pony Mail!
Pony Mail!
[SECURITY] Fedora 29 Update: nodejs-10.16.3-1.fc29 - package-announce - Fedora Mailing-Lists
Debian -- Security Information -- DSA-4509-1 apache2
Red Hat Customer Portal
Pony Mail!

September 2019 Apache HTTP Server Vulnerabilities in NetApp Products | NetApp Product Security

Pony Mail!

[SECURITY] Fedora 30 Update: mod_http2-1.15.3-2.fc30 - package-announce - Fedora Mailing-Lists

Pony Mail!

Pony Mail!

support.f5.com/csp/article/K02591030

CVE-2019-9517 Apache HTTP Server Vulnerability in NetApp Products | NetApp Product Security

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

McAfee Security Bulletin - Updates and product status for HTTP/2 vulnerabilities (CVE-2019-9511, CVE-2019-9512, CVE-2019-9513, CVE-20

Pony Mail!

[SECURITY] Fedora 30 Update: mod_http2-1.15.3-2.fc30 - package-announce - Fedora Mailing-Lists

USN-4113-1: Apache HTTP Server vulnerabilities | Ubuntu security notices | Ubuntu

August 2019 Node.js Vulnerabilities in NetApp Products | NetApp Product Security

Pony Mail!

Synology Inc.

[SECURITY] Fedora 29 Update: mod_http2-1.15.3-2.fc29 - package-announce - Fedora Mailing-Lists

oss-security - CVE-2019-9517: mod_http2, DoS attack by exhausting h2 workers

[security-announce] openSUSE-SU-2019:2115-1: important: Security update

Pony Mail!

Red Hat Customer Portal

Pony Mail!

security-bulletins/2019-002.md at master · Netflix/security-bulletins · GitHub

[SECURITY] Fedora 29 Update: nodejs-10.16.3-1.fc29 - package-announce - Fedora Mailing-Lists

Pony Mail!

[SECURITY] Fedora 30 Update: nodejs-10.16.3-1.fc30 - package-announce - Fedora Mailing-Lists

Apache: Multiple vulnerabilities (GLSA 201909-04) — Gentoo security

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Pony Mail!
[security-announce] openSUSE-SU-2019:2114-1: important: Security update
support.f5.com/csp/article/K02591030
Oracle Critical Patch Update - October 2019
Pony Mail!
Oracle Critical Patch Update Advisory - April 2020
Red Hat Customer Portal
[SECURITY] Fedora 30 Update: nodejs-10.16.3-1.fc30 - package-announce - Fedora Mailing-Lists
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Bugtraq: [SECURITY] [DSA 4509-1] apache2 security update
[security-announce] openSUSE-SU-2019:2051-1: important: Security update
VU#605641 - HTTP/2 implementations do not robustly handle abnormal traffic and resource exhaustion
Pony Mail!
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks to Jonathan Looney of Netflix for reporting this vulnerability.

Legacy QID Mappings

296079	Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)
377378	Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)
500018	Alpine Linux Security Update for apache2
500434	Alpine Linux Security Update for nodejs
503709	Alpine Linux Security Update for apache2
504197	Alpine Linux Security Update for nodejs
710128	Gentoo Linux Apache Multiple vulnerabilities (GLSA 201909-04)
940051	AlmaLinux Security Update for nodejs:10 (ALSA-2019:2925)

© 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 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.

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