



CVE-2019-9515

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-9515
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 a settings flood, potentially leading to a denial of service. The attacker ser

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	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	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	Graalvm	19.2.0	All	All	All
Application	Oracle	Graalvm	19.2.0	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 Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	4.1	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	Openstack	14	All	All	All
Application	Redhat	Openstack	14	All	All	All
Application	Redhat	Quay	3.0.0	All	All	All
Application	Redhat	Quay	3.0.0	All	All	All

Application	Redhat	Single Sign-on	7.3	All	All	All
Application	Redhat	Single Sign-on	7.3	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!

Red Hat Customer Portal

Bugtraq: [SECURITY] [DSA 4520-1] trafficserver security update

Red Hat Customer Portal

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

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

Full Disclosure: APPLE-SA-2019-08-13-5 SwiftNIO HTTP/2 1.5.0

Pony Mail!

Red Hat Customer Portal

Bugtraq: APPLE-SA-2019-08-13-5 SwiftNIO HTTP/2 1.5.0

Red Hat Customer Portal

myF5

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-2019-9514)

Red Hat Customer Portal

Red Hat Customer Portal

USN-4308-1: Twisted vulnerabilities | Ubuntu security notices | Ubuntu

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

Synology Inc.

Pony Mail!

Pony Mail!

Red Hat Customer Portal

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

Debian -- Security Information -- DSA-4508-1 h2o

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

support.f5.com/csp/article/K50233772

Red Hat Customer Portal

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

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

Red Hat Customer Portal

Debian -- Security Information -- DSA-4520-1 trafficserver

Bugtraq: [SECURITY] [DSA 4508-1] h2o security update

Red Hat Customer Portal

support.f5.com/csp/article/K50233772

[security-announce] openSUSE-SU-2019:2114-1: important: Security update

Red Hat Customer Portal

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

VU#605641 - HTTP/2 implementations do not robustly handle abnormal traffic and resource exhaustion

Red Hat Customer Portal

Red Hat Customer Portal

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)

[500434](#) Alpine Linux Security Update for nodejs

[500854](#) Alpine Linux Security Update for containerd

500995 Alpine Linux Security Update for h2o
501367 Alpine Linux Security Update for py3-twisted
504197 Alpine Linux Security Update for nodejs
504636 Alpine Linux Security Update for containerd
690329 Free Berkeley Software Distribution (FreeBSD) Security Update for h2o (73b1e734-c74e-11e9-8052-0028f8d09152)
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 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](#)