



# CVE-2019-9518

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

## Summary

<b>CVE</b>	CVE-2019-9518
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-08-13 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:13:00 UTC
<b>Description</b>	Some HTTP/2 implementations are vulnerable to a flood of empty frames, potentially leading to a denial of service. The attac

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Traffic Server</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Traffic Server</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Traffic Server</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Swiftnio</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Web Gateway</a>	All	All	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Web Gateway</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Application	<a href="#">Nodejs</a>	<a href="#">Node.js</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	19.2.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	19.2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Core Services</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Core Services</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Enterprise Application Platform</a>	7.2.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Enterprise Application Platform</a>	7.3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Enterprise Application Platform</a>	7.2.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Jboss Enterprise Application Platform</a>	7.3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Service Mesh</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Service Mesh</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Quay</a>	3.0.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Quay</a>	3.0.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Software Collections</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Software Collections</a>	1.0	All	All	All
Application	<a href="#">Synology</a>	<a href="#">Diskstation Manager</a>	6.2	All	All	All
Application	<a href="#">Synology</a>	<a href="#">Diskstation Manager</a>	6.2	All	All	All
Application	<a href="#">Synology</a>	<a href="#">Skynas</a>	-	All	All	All
Application	<a href="#">Synology</a>	<a href="#">Skynas</a>	-	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

[support.f5.com/csp/article/K46011592](https://support.f5.com/csp/article/K46011592)

Red Hat Customer Portal

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

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

[support.f5.com/csp/article/K46011592](https://support.f5.com/csp/article/K46011592)

Pony Mail!

Pony Mail!

Red Hat Customer Portal

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

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

Red Hat Customer Portal

McAfee Security Bulletin - Updates and product status for HTTP/2 vulnerabilities (CVE-2019-9511, CVE-2019-9512, CVE-2019-9513, CVE-2019-9514)

Pony Mail!

Pony Mail!

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

Synology Inc.

Pony Mail!

Red Hat Customer Portal

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

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

Pony Mail!

Pony Mail!

myF5

Pony Mail!

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

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

Pony Mail!

Red Hat Customer Portal

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

Pony Mail!

Pony Mail!

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

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail



### Vendor Comments And Credit

Discovery Credit

**LEGACY:** Thanks to Piotr Sikora of Google for reporting this vulnerability.

### Legacy QID Mappings

<a href="#">296079</a> Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)
<a href="#">500434</a> Alpine Linux Security Update for nodejs
<a href="#">504197</a> Alpine Linux Security Update for nodejs
<a href="#">940051</a> 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](#)