



# CVE-2019-9516

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-9516
<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 header leak, potentially leading to a denial of service. The attacker sends

## 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
Application	<a href="#">F5</a>	<a href="#">Nginx</a>	All	All	All	All
Application	<a href="#">F5</a>	<a href="#">Nginx</a>	All	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>	32	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>	32	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="#">Nginx</a>	<a href="#">Nginx</a>	All	All	All	All
Application	<a href="#">Nginx</a>	<a href="#">Nginx</a>	All	All	All	All
Application	<a href="#">Nginx</a>	<a href="#">Nginx</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	<a href="#">Synology</a>	<a href="#">Vs960hd</a>	-	All	All	All
Hardware	<a href="#">Synology</a>	<a href="#">Vs960hd</a>	-	All	All	All
Operating System	<a href="#">Synology</a>	<a href="#">Vs960hd Firmware</a>	-	All	All	All
Operating System	<a href="#">Synology</a>	<a href="#">Vs960hd Firmware</a>	-	All	All	All

## References

### Reference

[Red Hat Customer Portal](#)

[myF5](#)

[Red Hat Customer Portal](#)

[\[SECURITY\] Fedora 29 Update: mod\\_http2-1.15.3-2.fc29 - package-announce - Fedora Mailing-Lists](#)

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

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[\[SECURITY\] Fedora 30 Update: mod\\_http2-1.15.3-2.fc30 - package-announce - Fedora Mailing-Lists](#)

[support.f5.com/csp/article/K02591030](https://support.f5.com/csp/article/K02591030)

[Red Hat Customer Portal](#)

[Full Disclosure: APPLE-SA-2019-08-13-5 SwiftNIO HTTP/2 1.5.0](#)

[Red Hat Customer Portal](#)

[Bugtraq: APPLE-SA-2019-08-13-5 SwiftNIO HTTP/2 1.5.0](#)

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

[USN-4099-1: nginx vulnerabilities | Ubuntu security notices | Ubuntu](#)

[\[SECURITY\] Fedora 30 Update: mod\\_http2-1.15.3-2.fc30 - package-announce - Fedora Mailing-Lists](#)

[\[security-announce\] openSUSE-SU-2019:2120-1: important: Security update](#)

[\[SECURITY\] Fedora 29 Update: nginx-1.16.1-1.fc29 - package-announce - Fedora Mailing-Lists](#)

[August 2019 Node.js Vulnerabilities in NetApp Products | NetApp Product Security](#)

[Red Hat Customer Portal](#)

[\[SECURITY\] Fedora 32 Update: nodejs-12.20.1-1.fc32 - package-announce - Fedora Mailing-Lists](#)

[Synology Inc.](#)

[\[SECURITY\] Fedora 30 Update: nginx-1.16.1-1.fc30 - package-announce - Fedora Mailing-Lists](#)

[\[SECURITY\] Fedora 29 Update: mod\\_http2-1.15.3-2.fc29 - package-announce - Fedora Mailing-Lists](#)

[SECURITY] Fedora 30 Update: nginx-1.16.1-1.fc30 - package-announce - Fedora Mailing-Lists

August 2019 NGINX Vulnerabilities in NetApp Products | NetApp Product Security

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

Red Hat Customer Portal

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

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

Red Hat Customer Portal

[security-announce] openSUSE-SU-2019:2264-1: moderate: Security update f

Red Hat Customer Portal

Debian -- Security Information -- DSA-4505-1 nginx

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

support.f5.com/csp/article/K02591030

Bugtraq: [SECURITY] [DSA 4505-1] nginx security update

Red Hat Customer Portal

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

[SECURITY] Fedora 29 Update: nginx-1.16.1-1.fc29 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 32 Update: nodejs-12.20.1-1.fc32 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

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 Jonathan Looney of Netflix 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="#">377103</a> Alibaba Cloud Linux Security Update for nginx:1.20 (ALINUX3-SA-2022:0016)
<a href="#">377378</a> Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)
<a href="#">500427</a> Alpine Linux Security Update for nginx
<a href="#">500434</a> Alpine Linux Security Update for nodejs

504186 Alpine Linux Security Update for nginx
504197 Alpine Linux Security Update for nodejs
900026 CBL-Mariner Linux Security Update for nginx 1.16.1
902950 Common Base Linux Mariner (CBL-Mariner) Security Update for nginx (3590)
940051 AlmaLinux Security Update for nodejs:10 (ALSA-2019:2925)
940134 AlmaLinux Security Update for nginx:1.14 (ALSA-2019:2799)
960386 Rocky Linux Security Update for nodejs:10 (RLSA-2019:2925)
960857 Rocky Linux Security Update for nginx:1.14 (RLSA-2019:2799)

© [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](#)**