CVE-2019-9511

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-9511
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 window size manipulation and stream prioritization manipulation, potential

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	Nginx	All	All	All	All
Application	F5	Nginx	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	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	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	Enterprise Communications Broker	3.1.0	All	All	All
Application	Oracle	Enterprise Communications Broker	3.2.0	All	All	All
Application	Oracle	Enterprise Communications Broker	3.1.0	All	All	All
Application	Oracle	Enterprise Communications Broker	3.2.0	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 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
[SECURITY] Fedora 29 Update: nghttp2-1.39.2-1.fc29 - package-announce - Fedora Mailing-Lists
myF5
Red Hat Customer Portal
[SECURITY] Fedora 29 Update: mod_http2-1.15.3-2.fc29 - package-announce - Fedora Mailing-Lists
Red Hat Customer Portal
Debian -- Security Information -- DSA-4669-1 nodejs
Red Hat Customer Portal
[SECURITY] Fedora 30 Update: mod_http2-1.15.3-2.fc30 - package-announce - Fedora Mailing-Lists
Red Hat Customer Portal
support.f5.com/csp/article/K02591030
Red Hat Customer Portal
Red Hat Customer Portal
[SECURITY] Fedora 29 Update: nghttp2-1.39.2-1.fc29 - package-announce - Fedora Mailing-Lists
Oracle Critical Patch Update Advisory - October 2020
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-20
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
Debian -- Security Information -- DSA-4511-1 nghttp2

Red Hat Customer Portal

[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

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

Red Hat Customer Portal

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

Red Hat Customer Portal

[SECURITY] Fedora 30 Update: nghttp2-1.39.2-1.fc30 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

[security-announce] openSUSE-SU-2019:2232-1: moderate: Security update f

Bugtraq: [SECURITY] [DSA 4511-1] nghttp2 security update

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

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

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

support.f5.com/csp/article/K02591030

Oracle Critical Patch Update - October 2019

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

Red Hat Customer Portal

[SECURITY] Fedora 30 Update: nghttp2-1.39.2-1.fc30 - package-announce - Fedora Mailing-Lists

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

Red Hat Customer Portal

Oracle Critical Patch Update Advisory - January 2021

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

Red Hat Customer Portal

[security-announce] openSUSE-SU-2019:2234-1: moderate: Security update f

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

- 174904 SUSE Enterprise Linux Security Update for nghttp2 (SUSE-SU-2021:0932-1)
- 296079 Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)
- 377103 Alibaba Cloud Linux Security Update for nginx:1.20 (ALINUX3-SA-2022:0016)
- 377378 Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)
- 500423 Alpine Linux Security Update for nghttp2
- 500427 Alpine Linux Security Update for nginx
- 500434 Alpine Linux Security Update for nodejs
- 504182 Alpine Linux Security Update for nghttp2
- 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
- 902808 Common Base Linux Mariner (CBL-Mariner) Security Update for nginx (3594)
- 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)