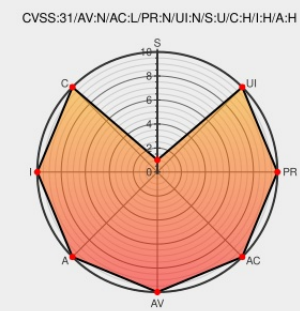
CVE-2020-1944

Published on: 03/23/2020 12:00:00 AM UTC

Last Modified on: 10/06/2022 08:36:00 PM UTC

CVE-2020-1944

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Traffic Server from Apache contain the following vulnerability:

There is a vulnerability in Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.8, and 8.0.0 to 8.0.5 with a smuggling attack and Transfer-Encoding and Content length headers. Upgrade to versions 7.1.9 and 8.0.6 or later versions.

CVE-2020-1944 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4672-1	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-4672

trafficserver

Pony Mail! Mailing List Vendor Advisory lists.apache.org text/html MISC lists.apache.org/thread.html/r99d18d0bc4daa05e7d0e5a63e0e22701a421b2ef5a8f4f7694c43869%40%3Ca

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	Debian	Debian Linux	10.0	All	All	All

cpe:2.3:a:apache:traffic_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:traffic_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:traffic_server:*:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID Next ID→