



# CVE-2021-44040

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

## Summary

<b>CVE</b>	CVE-2021-44040
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-23 14:15:00 UTC
<b>Updated</b>	2022-10-14 11:40:00 UTC
<b>Description</b>	Improper Input Validation vulnerability in request line parsing of Apache Traffic Server allows an attacker to send invalid rec

## Risk And Classification

**Problem Types:** CWE-20

## 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
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>	11.0	All	All	All

## References

Reference	Source	Link	Tags
N/A	CONFIRM	<a href="https://lists.apache.org">lists.apache.org</a>	
Debian -- Security Information -- DSA-5153-1 trafficserver	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Apache Traffic Server would like to thank Bahruz Jabiyev, Steven Sprecher and Kaan Onarlioglu for reporting these issues. We used his tool t-reqs (<https://github.com/bahruzjabiyev/t-reqs-http-fuzzer>) for discovering them.

## Legacy QID Mappings

[179337](#) Debian Security Update for trafficserver (DSA 5153-1)

[184579](#) Debian Security Update for trafficserver (CVE-2021-44040)

[87491](#) Apache Traffic Server Multiple Vulnerabilities

© [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](#)