



# CVE-2018-8004

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

## Summary

<b>CVE</b>	CVE-2018-8004
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-29 13:29:00 UTC
<b>Updated</b>	2023-11-07 03:01:00 UTC
<b>Description</b>	There are multiple HTTP smuggling and cache poisoning issues when clients making malicious requests interact with Apac

## Risk And Classification

**Problem Types:** CWE-444

## 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>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All

## References

### Reference

Pony Mail!

Debian -- Security Information -- DSA-4282-1 trafficserver

Close the connection when returning a 400 error response by bryancall · Pull Request #3201 · apache/trafficserver · GitHub

Apache Traffic Server CVE-2018-8004 Multiple Security Vulnerabilities

Pony Mail!

Return 400 if there is whitespace after the field name and before the colon by bryancall · Pull Request #3192 · apache/trafficserver · GitHub

Drain the request body if there is a cache hit by bryancall · Pull Request #3251 · apache/trafficserver · GitHub

Validate Content-Length headers for incoming requests by bryancall · Pull Request #3231 · apache/trafficserver · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)