



CVE-2015-3249

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

Summary

CVE	CVE-2015-3249
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-30 14:29:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	The HTTP/2 experimental feature in Apache Traffic Server 5.3.x before 5.3.1 allows remote attackers to cause a denial of s

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Traffic Server	5.3.0	All	All	All
Application	Apache	Traffic Server	5.3.0	All	All	All

References

Reference	Source	Link	Tags
Apache Traffic Server - HTTP2 Fuzzing Yahoo Security	MISC	yahoo-security.tumblr.com	Issue Tr
[ANNOUNCE] Apache Traffic Server 5.3.1 is released!		mail-archives.us.apache.org	
Apache Traffic Server CVE-2015-3249 Multiple Remote Code Execution Vulnerabilities	BID	www.securityfocus.com	Third Pa
[ANNOUNCE] Apache Traffic Server 5.3.1 is released!	MLIST	mail-archives.us.apache.org	Issue Tr
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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](#)