



CVE-2017-7670

Published on: 07/10/2017 12:00:00 AM UTC

Last Modified on: 06/16/2021 09:15:00 PM UTC

CVE-2017-7670

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Traffic Control](#) from [Apache](#) contain the following vulnerability:

The Traffic Router component of the incubating Apache Traffic Control project is vulnerable to a Slowloris style Denial of Service attack. TCP connections made on the configured DNS port will remain in the ESTABLISHED state until the client explicitly closes the connection or Traffic Router is restarted. If connections remain in the ESTABLISHED

state indefinitely and accumulate in number to match the size of the thread pool dedicated to processing DNS requests, the thread pool becomes exhausted. Once the thread pool is exhausted, Traffic Router is unable to service any DNS request, regardless of transport protocol.

CVE-2017-7670 has been assigned by security@apache.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Apache Software Foundation](#) - [Apache Traffic Control](#) version **1.8.0 incubating**

Affected Vendor/Software: [Apache Software Foundation](#) - [Apache Traffic Control](#) version **2.0.0 RC0 incubating**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

PARTIAL

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	 MLIST [trafficcontrol-commits] 20190906 [trafficcontrol-website] branch asf-site updated: Adds CVE-2019-12405 to security page
Pony Mail!	lists.apache.org text/html	 MLIST [trafficcontrol-commits] 20210616 [trafficcontrol-website] branch asf-site updated: Fix CVE-2020-17522 link
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [users] 20170707 Apache Traffic Control Traffic Router Slowloris Denial of Service Vulnerability - CVE-2017-7670

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 Control	1.8.1	rc0	All	All
Application	Apache	Traffic Control	2.0.0	rc1	All	All
Application	Apache	Traffic Control	2.0.0	rc2	All	All
Application	Apache	Traffic Control	2.0.0	rc3	All	All
Application	Apache	Traffic Control	2.0.0	rc4	All	All
Application	Apache	Traffic Control	2.0.0	rc5	All	All
Application	Apache	Traffic Control	2.0.0	rc6	All	All
Application	Apache	Traffic Control	1.8.1	rc0	All	All
Application	Apache	Traffic Control	2.0.0	rc1	All	All
Application	Apache	Traffic Control	2.0.0	rc2	All	All
Application	Apache	Traffic Control	2.0.0	rc3	All	All
Application	Apache	Traffic Control	2.0.0	rc4	All	All
Application	Apache	Traffic Control	2.0.0	rc5	All	All
Application	Apache	Traffic Control	2.0.0	rc6	All	All
Application	Apache	Traffic Control	All	All	All	All
cpe:2.3:a:apache:traffic_control:1.8.1:rc0:*****:						
cpe:2.3:a:apache:traffic_control:2.0.0:rc1:*****:						
cpe:2.3:a:apache:traffic_control:2.0.0:rc2:*****:						

cpe:2.3:a:apache:traffic_control:2.0.0:rc2:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc3:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc4:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc5:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc6:*****:
cpe:2.3:a:apache:traffic_control:1.8.1:rc0:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc1:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc2:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc3:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc4:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc5:*****:
cpe:2.3:a:apache:traffic_control:2.0.0:rc6:*****:
cpe:2.3:a:apache:traffic_control:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)