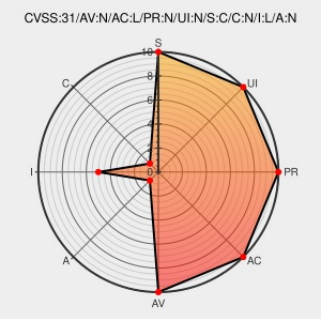
CVE-2020-17522

Published on: 01/26/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:19:00 AM UTC

CVE-2020-17522

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



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

When ORT (now via atstccfg) generates ip_allow.config files in Apache Traffic Control 3.0.0 to 3.1.0 and 4.0.0 to 4.1.0, those files include permissions that allow bad actors to push arbitrary content into and remove arbitrary content from CDN cache servers. Additionally, these permissions are potentially extended to IP addresses outside the desired range, resulting in them being granted to clients possibly outside the CDN arcitechture.

CVE-2020-17522 has been assigned by security@apache.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.8 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Repy Mail		MLIST [trafficcontrol-commits] 20210616 [trafficcontrol-website] branch asf-site updated: Fix CVE-2020-1

Pony Mail!	lists.apache.org text/html	MLIST [trafficcontrol-commits] 20210616 [trafficcontrol-website] branch asf-site updated: Fix CVE-2020-1
Pony Mail!	lists.apache.org text/html	MLIST [trafficcontrol-commits] 20211011 [trafficcontrol-website] 01/02: Add CVE-2021-42009
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MISC lists.apache.org/thread.html/r3de212a3da73bcf98fa2db7eafb75b2eb8e131ff466e6efc4284df09%40%3Cdev

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for exploiting CVE-2020-17522 : When ORT (now via atstccfg) generates ip_allow.config files in Apache Traffic Con…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Traffic Control	All	All	All	All
Application	Apache	Traffic Control	All	All	All	All

cpe:2.3:a:apache:traffic_control:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:traffic_control:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Apache - CVE-2020-17522: lists.apache.org/thread.html/r3…	2021-06-16 22:45:21

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report