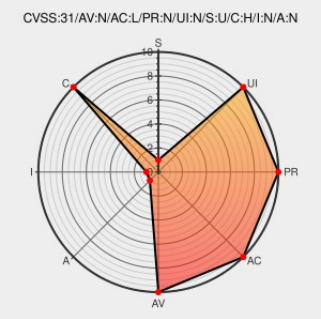
CVE-2022-23206

Published on: 02/06/2022 12:00:00 AM UTC

Last Modified on: 02/11/2022 03:16:00 AM UTC

CVE-2022-23206

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



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

In Apache Traffic Control Traffic Ops prior to 6.1.0 or 5.1.6, an unprivileged user who can reach Traffic Ops over HTTPS can send a specially-crafted POST request to /user/login/oauth to scan a port of a server that Traffic Ops can reach.

CVE-2022-23206 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 **< 6.1.0**

Affected Vendor/Software: **Apache Software Foundation** - **Apache Traffic Control** version **< 5.1.6**

Vulnerability Patch/Work Around

6.0.x user should upgrade to 6.1.0. 5.1.x users should upgrade to 5.1.6 or 6.1.0.

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	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/lsrd2mqj29vrvwsh8g0d560vvz8n126f

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.

Related QID Numbers

376439 Apache Traffic Control Server-Side Request Forgery (SSRF) Vulnerability

Known Affected Configurations (CPE V2.3)

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

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

Discovery Credit

Apache Traffic Control would like to thank walkerxiong of SecCoder Security Lab for reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23206 : In #Apache Traffic Control Traffic Ops prior to 6.1.0 or 5.1.6, an unprivileged user who can reach… twitter.com/i/web/status/1…	2022-02-06 15:20:57
/r/netcve	CVE-2022-23206	2022-02-06 16:38:18

← Previous ID

Next ID→