



# 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>NONE</b>         |

## CVE References

| Description             | Tags                                                          | Link                                                                                                                                                                                                                         |
|-------------------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No Description Provided | <a href="#">lists.apache.org</a><br><a href="#">text/html</a> |  <a href="https://lists.apache.org/thread/lsrc2mqj29vrwsh8g0d560vvz8n126f">MISC lists.apache.org/thread/lsrc2mqj29vrwsh8g0d560vvz8n126f</a> |

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](mailto: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                             | <a href="#">Apache</a> | <a href="#">Traffic Control</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-02-06 15:20:57 |
|  /r/netcve  | <a href="#">CVE-2022-23206</a>                                                                                                                                                                           | 2022-02-06 16:38:18 |

[← 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](#)