



# CVE-2023-31426

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2023-31426  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | sirt@brocade.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2023-08-01 22:15:00 UTC   |
| <b>Updated</b>         | 2023-09-08 17:15:00 UTC   |
| <b>Description</b>     | The Brocade Fabric OS Commands "configupload" and "configdownload" before Brocade Fabric OS v9.1.1c, v8.2.3d, v9.2. |

## Risk And Classification

**Problem Types:** CWE-532

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor   | Product                 | Version | Update | Edition | Language |
|------------------|----------|-------------------------|---------|--------|---------|----------|
| Operating System | Broadcom | Fabric Operating System | All     | All    | All     | All      |

## References

| Reference   | Source  | Link  | Tags                |
|---|---------|---|---------------------|
| August 2023 Brocade Fabric OS Vulnerabilities   NetApp Product Security | MISC    | <a href="https://security.netapp.com">security.netapp.com</a>   |                     |
| Support Content Notification - Support Portal - Broadcom support portal | MISC    | <a href="https://support.broadcom.com">support.broadcom.com</a> |                     |
| CVE Program record  | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                   | canonical           |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                 | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)