



# CVE-2022-28167

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-28167
<b>State</b>	PUBLIC
<b>Assigner</b>	sirt@brocade.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-27 18:15:00 UTC
<b>Updated</b>	2023-08-08 14:22:00 UTC
<b>Description</b>	Brocade SANnav before Brocade SANnav v. 2.2.0.2 and Brocade SANnav v.2.1.1.8 logs the Brocade Fabric OS switch pas

## Risk And Classification

**Problem Types:** CWE-522

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Sannav	All	All	All	All

## References

Reference	Source	Link	Tags
BSA-2022-1978	MISC	<a href="http://www.broadcom.com">www.broadcom.com</a>	
CVE-2022-28167 Brocade SANnav Vulnerability   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
CVE Program record	CVE.ORG	<a href="http://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)