



CVE-2023-1096

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

Summary

CVE	CVE-2023-1096
State	PUBLIC
Assigner	security-alert@netapp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-12 21:15:00 UTC
Updated	2023-05-24 16:53:00 UTC
Description	SnapCenter versions 4.7 prior to 4.7P2 and 4.8 prior to 4.8P1 are susceptible to a vulnerability which could allow a remote

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Snapcenter	4.7	-	All	All
Application	Netapp	Snapcenter	4.7	p1	All	All
Application	Netapp	Snapcenter	4.8	-	All	All

References

Reference	Source	Link	Tags
CVE-2023-1096 Authentication Bypass Vulnerability in SnapCenter NetApp Product Security	MISC	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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