



CVE-2022-20777

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

Summary

CVE	CVE-2022-20777
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-04 17:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an attacker to escape from the

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Enterprise Nfv Infrastructure Software	All	All	All	All

References

Reference	Source
Cisco Enterprise NFVIS - Improper Access Control in NFVIS (CVE-2022-20777) · Advisory · orangecertcc/security-research · GitHub	MISC
20220504 Cisco Enterprise NFV Infrastructure Software Vulnerabilities	CISCO
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)