



CVE-2023-37249

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-37249
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-25 20:15:00 UTC
Updated	2023-08-31 18:12:00 UTC
Description	Infoblox NIOS through 8.5.1 has a faulty component that accepts malicious input without sanitization, resulting in shell acce

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Infoblox	Nios	All	All	All	All

References

Reference	Source	Link	Tags
Infoblox Simplify & Unite Networking and Security	MISC	infoblox.com	
NIOS is vulnerable to CVE-2023-37249 - Infoblox Experts Community	CONFIRM	community.infoblox.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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

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