



CVE-2023-30799

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

Summary

CVE	CVE-2023-30799
State	PUBLIC
Assigner	disclosure@vulncheck.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-19 15:15:00 UTC
Updated	2023-07-28 13:47:00 UTC
Description	MikroTik RouterOS stable before 6.49.7 and long-term through 6.48.6 are vulnerable to a privilege escalation issue. A remote

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Mikrotik	Routers	All	All	All	All
Operating System	Mikrotik	Routers	All	All	All	All

References

Reference	Source	Link	Tags
GitHub - MarginResearch/FOISted: MikroTik remote jailbreak for v6.x.x	MISC	github.com	
MikroTik RouterOS Administrator Privilege Escalation VulnCheck Advisories	MISC	vulncheck.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.

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](#).

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