CVE-2021-3014

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3014
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-04 19:15:00 UTC
Updated	2021-01-07 21:33:00 UTC
Description	In MikroTik RouterOS through 2021-01-04, the hotspot login page is vulnerable to reflected XSS via the target parameter.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
MikroTik hotspot login XSS | M0e	MISC	m4dm0e.github.io
m4dm0e.github.io/2021-01-04-mikrotik-xss-reflected.md at gh-pages · M4DM0e/m4dm0e.github.io · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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