



CVE-2019-3978

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

Summary

CVE	CVE-2019-3978
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-29 19:15:00 UTC
Updated	2019-11-01 14:46:00 UTC
Description	RouterOS versions 6.45.6 Stable, 6.44.5 Long-term, and below allow remote unauthenticated attackers to trigger DNS quer

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
MikroTik RouterOS 6.45.6 DNS Cache Poisoning ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Advisory
MikroTik RouterOS Multiple Vulnerabilities - Research Advisory Tenable®	MISC	www.tenable.com	Third Party Advisory
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](#).

Free CVE JSON API cve.report/api

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