



CVE-2018-10066

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

Summary

CVE	CVE-2018-10066
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-13 13:29:00 UTC
Updated	2018-05-17 17:15:00 UTC
Description	An issue was discovered in MikroTik RouterOS 6.41.4. Missing OpenVPN server certificate verification allows a remote unauthenticated user to execute arbitrary code on the target system.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mikrotik	Routeros	6.41.4	All	All	All
Application	Mikrotik	Routeros	6.41.4	All	All	All

References

Reference	Source	Link	Tags
404 Not Found	MISC	janis-streib.de	Exploit, 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.

Legacy QID Mappings

[730288](#) MikroTik RouterOS Open Virtual Private Network (OpenVPN) Server Certificate Verification Vulnerability

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