CVE-2018-14847

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-14847
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-02 07:29:00 UTC
Updated	2019-03-07 14:12:00 UTC
Description	MikroTik RouterOS through 6.42 allows unauthenticated remote attackers to read arbitrary files and remote authenticated a

Risk And Classification

EPSS: 0.936450000 probability, percentile 0.998470000 (date 2026-05-16)

CISA KEV: Listed on 2021-12-01; due 2022-06-01; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	MikroTik
Product	RouterOS
Name	MikroTik Router OS Directory Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-14847

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
Dissection of Winbox critical vulnerability	MISC	n0p.me
GitHub - BigNerd95/WinboxExploit: Proof of Concept of Winbox Critical Vulnerability	MISC	github.com
GitHub - BasuCert/WinboxPoC: Proof of Concept of Winbox Critical Vulnerability (CVE-2018-14847)	MISC	github.com
MicroTik RouterOS < 6.43rc3 - Remote Root - Hardware remote Exploit	EXPLOIT-DB	www.exploit-db.com

routeros/poc/cve_2018_14847 at master · tenable/routeros · GitHub	MISC	github.com
routeros/bug_hunting_in_routeros_derbycon_2018.pdf at master · tenable/routeros · GitHub	MISC	github.com
routeros/poc/bytheway at master · tenable/routeros · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

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