

CVE-2018-7445

MikroTik RouterOS Stack-Based Buffer Overflow Vulnerability

CISA KEV since Sep 8, 2022

Actively exploited

A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages. Remote attackers with access to the service can exploit this vulnerability and gain code execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it. All architectures and all devices running RouterOS before versions 6.41.3/6.42rc27 are vulnerable.

EVRS 77/₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.608 99.15th percentile · FIRST	CISA DEADLINE Sep 29, 2022 KEV since 2022 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.608 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
routeros	< 6.41.3 6.42	6.41.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-v596-x9hf-63gj

coresecurity.com coresecurity.com/core-labs/advisories/mikrotik-routeros-smb-buffer-overflow#vendor_update, <https://mikrotik.com/download>

NVD nvd.nist.gov/vuln/detail/CVE-2018-7445

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-19176

Current data evulnable.com/vulnerability-management/cve/CVE-2018-7445

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.