CVE-2018-7445

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

Summary

CVE	CVE-2018-7445
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-19 21:29:00 UTC
Updated	2018-04-24 14:53:00 UTC
Description	A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages.

Risk And Classification

EPSS: 0.875570000 probability, percentile 0.994700000 (date 2026-05-08)

CISA KEV: Listed on 2022-09-08; due 2022-09-29; ransomware use Unknown

Problem Types: CWE-119

CISA Known Exploited Vulnerability

Vendor	MikroTik
Product	RouterOS
Name	MikroTik RouterOS Stack-Based Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://www.coresecurity.com/core-labs/advisories/mikrotik-routeros-smb-buffer-overflow#vendor_update, https://mikrotik.com/download; https://nvd.nist.gov/vuln/detail/CVE-2018-7445

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	6.4.2	rc11	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc12	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc14	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc15	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc18	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc2	All	All

Operating System	Mikrotik	Routeros	6.4.2	rc20	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc23	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc24	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc27	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc5	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc6	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc9	All	All
Operating System	Mikrotik	Routeros	All	All	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc11	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc12	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc14	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc15	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc18	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc2	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc20	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc23	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc24	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc27	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc5	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc6	All	All
Operating System	Mikrotik	Routeros	6.4.2	rc9	All	All

References

Reference	Source	Link	Tags
Full Disclosure: [CORE-2018-0003] MikroTik RouterOS SMB Buffer Overflow	FULLDISC	seclists.org	Exploit, M
MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow - Hardware remote Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, T
MikroTik RouterOS CVE-2018-7445 Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Par
MikroTik RouterOS SMB Buffer Overflow | Core Security	MISC	www.coresecurity.com	Exploit, T
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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