Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0345

Kwetsbaarheden verholpen in MikroTik RouterOS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-09-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

MikroTik heeft meerdere kwetsbaarheden verholpen in RouterOS.

Duiding

De eerste kwetsbaarheid betreft een fout in de SSH-authenticatiemechanisme waarbij de exponent van RSA-sleutels niet werd geverifieerd. Hierdoor kunnen aanvallers RSA-handtekeningen vervalsen en ongeautoriseerde SSH-toegang verkrijgen. De tweede kwetsbaarheid betreft een probleem met gebruikersnamen die beginnen met een verboden teken, waardoor de trusted policy mask kan worden gemanipuleerd en privilege escalation mogelijk is binnen het SSH-loginproces. De derde kwetsbaarheid maakt het mogelijk voor niet-geauthenticeerde clients om een IPv4 UDP-test te starten die door onjuiste verwerking van pakketten in de kernel kan leiden tot kernel restarts, wat de beschikbaarheid van het systeem beïnvloedt.

CERT Polen geeft aan actief misbruik te hebben waargenomen, gericht op routers waarbij de SSH service publiek toegankelijk is. In deze gevallen zijn meerdere van bovenstaande kwetsbaarheden gecombineerd om volledige controle over de getroffen routers te verkrijgen. Het is goed gebruik om SSH toegang niet open te stellen aan het internet, maar af te schermen via een VPN en/of whitelist.

Oplossingen

MikroTik heeft updates uitgebracht in RouterOS versies 6.49.21, 7.23.4 en 7.24.2 om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://cert.pl/en/posts/2026/09/vulnerabilities-in-mikrotik-routeros-actively-exploited/
- https://mikrotik.com/supportsec/september-2026-vulnerability/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-67276	9.2 CRITICAL
CVE-2026-86060	9.2 CRITICAL
CVE-2026-67277	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-306	Missing Authentication for Critical Function
CWE-347	Improper Verification of Cryptographic Signature

Getroffen producten

MikroTik
RouterOS

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.