CVE-2025-42611 – Authentication bypass in multiple RouterOS services caused by improper certificate validation

Summary

RouterOS provides various services that rely on correct verification of client and server certificates to secure confidentiality and integrity of communications. This includes OpenVPN, CAPsMAN, Dot1x (802.1X), among others.

The vulnerability lies in shared certificate validation logic which uses the system certificate store that is shared and equally trusted by all system services. This causes confusion of scope, allowing any certificate authority present in the system-wide trust store to be trusted in any context (with some exceptions), allowing partial or full authentication bypass in CAPsMAN, OpenVPN, Dot1X and potentially others. Manual intervention is required to fully resolve this vulnerability.

The most exploitable system configuration is present in systems that have been configured to trust public certificate authorities in order to securely connect to external systems (required for TLS/HTTPS-protected fetch tool, DoH, adlist, email, MQTT, LoRA, Netwatch).

In this configuration an attacker can obtain any non-expired X.509 certificate signed by any public CA (e.g. Let’s Encrypt) for any domain and use it to completely bypass CAPsMAN server and client authentication, OpenVPN server and client certificate authentication (but not password authentication), and 802.1X server certificate authentication, potentially leading to full loss of confidentiality or integrity of these services.

Identifiers

CVE-2025-42611
Vendor: Mikrotik
Product: RouterOS
Vulnerability: Weakness of certificate
CWE-923: Improper Restriction of Communication Channel to Intended Endpoints
CWE-295: Improper Certificate Validation
Affected versions: RouterOS 7.20.x and lower
CVSSv3.1: 6.5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Vulnerable products

All RouterOS releases 7.20 and earlier are affected by this vulnerability.

The vulnerability has been addressed in RouterOS 7.21. Users are strongly advised to upgrade to this version or later to ensure improved certificate validation – manual intervention is required.

Versions 7.21 and above still suffer from the vulnerability but changes have been made to make it significantly less exploitable in most environments, depending on overall system configuration.

Details

The vulnerability exploits the fact that RouterOS certificate validation logic components do not properly validate whether the presented certificate is signed by the expected CA. Instead, they implicitly trusts any CA present in the system’s certificate store.

As a result, CAs that are meant to be trusted in one context (e.g. to validate server certificates in TLS communication) are also trusted in others contexts (e.g. validation of client certificates in CAPsMAN and OpenVPN). These alternate contexts either don’t support or don’t enforce CN or SAN verification, allowing an arbitrary X.509 certificate (e.g. certificate for www.example.com signed by Let’s Encrypt) to be used to bypass authentication in CAPsMAN or OpenVPN.

It’s expected that every service that uses certificates for authentication would be bound to specific, pinned, CA certificate. For example, an OpenVPN server for employees should only accept certificates signed by “Employee VPN CA” and verify that the CN in the certificates matches their username. CAPsMAN server should only accept certificates signed by our chosen “internal Network CA” and it should verify the presence of certificate EKU fields as required by 2.4.4.3. of RFC 5415.

Impact

The impact is highly dependent on the overall system configuration and this list is not exhaustive, however by exploiting this flaw, an attacker can potentially:

- impersonate a CAP and obtain wireless configuration data intended only for authorized access points (SSIDs, passwords, VLAN assignments),
- impersonate a CAPsMAN server and reconfigure access points,
- impersonate the 802.1X server and gain access to switch ports,
- partially bypass OpenVPN client authentication (username/password might be required)
- impersonate an OpenVPN server

These actions can allow an attacker to gain or expand their foothold inside the network.

Exploitation status

There are currently no known exploits in circulation that target this vulnerability.

Mitigation

Manual review is required:

- Users should upgrade to RouterOS >= 7.21.
- All existing user-imported certificates will have their `trust-store` set to `all` after the upgrade, leaving them open to abuse until their scope is manually restricted
- Review every manually-imported certificate, and remove all `trust-store` values except those applicable to the certificate
- **Review any certificate import scripts that might be in use**. The default `trust-store` parameter for the certificate import command is `all` which could make the system vulnerable again.

Documentation:

- https://help.mikrotik.com/docs/spaces/ROS/pages/2555969/Certificates#Certificates-Certificateproperties
- https://help.mikrotik.com/docs/spaces/ROS/pages/2555969/Certificates#Certificates-ImportCertificate

Additionally:

- Exploitation of this vulnerability requires an on-path attacker, use strong network segmentation for sensitive services (e.g. CAPsMAN)
- Design the system with the understanding that all services of the same type share the same certificate store. It's currently impossible to ensure that certificates for one OpenVPN server aren't accepted by another OpenVPN server. Don't rely on certificates as the only authentication factor.

Contact

SI-CERT
ARNES
Tehnološki park 18, 1000 Ljubljana
T: 01 479 88 00
E: info@cert.si

READ ALSO

NEWS / 17. 4. 2026

CVE-2026-25599 – Insufficient neutralization of device-supplied input on the Orca user portal

Summary A critical security vulnerability has been identified in the Orca user portal, resulting from the way the portal processes data received from Orca devices. Because the older Orca devices ...

MORE →

NEWS / 24. 2. 2026

VANTAGE – Vulnerability Assessment aNd Testing Automation for Global Enhancement

Project coordinator Diadikasia Business Consulting Symvouloi Epicheiriseon AE Diadikasia Business Consultants SA, GR Project partners Project duration 1 January 2026 – 31 December 2028 (36 months) Summary VANTAGE (Vulnerability Assessment ...

MORE →

EU PROJEKTI,NEWS / 21. 1. 2025

INTERCEPT – IncideNt ThrEat shaRing CybErsecurity PlaTform

Project coordinator: T-2, Družba za ustvarjanje razvoj in trženje elektronskih komunikacij in opreme d. o. o., Slovenia Contact details: intercept@t-2.com Project partners: T-2 d. o. o., Družba za ustvarjanje ...

MORE →