GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

5 August 2026

Advisory 179: N-able N-central Authentication Bypass and Administrative Account Takeover Actively Exploited (CVE-2026-18556 and CVE-2026-18577).

Release Date: 4th August 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

N-able N-central contains two related Authentication Bypass Using an Alternate Path or Channel vulnerabilities (CWE-288, CVSS v4.0 8.2 each), which allow a remote, unauthenticated attacker to bypass authentication controls and take over user accounts, including accounts holding full administrative privileges, on a vulnerable N-central server. These advisory covers both issues, which form a single exploitation campaign and share the same remediation.

CVE-2026-18556, titled by the vendor as "unauthenticated administrative account takeover", was disclosed on 1 August 2026 following observed exploitation. N-able stated that the issue had already been addressed in N-central 2026.2, released on 28 April 2026, and initially advised customers on earlier versions to upgrade to 2026.3 as an immediate protective measure.

CVE-2026-18577 arises from that fix being incomplete. On 2 August 2026 N-able identified an alternative method of exploiting the same weakness which the 2026.2 fix did not block, issued the

finding as a second CVE, and released an emergency hotfix. This extended the affected range to all builds prior to 2026.3.1.7.

What are the systems affected?

The vulnerabilities affect N-able N-central across the following versions:

- CVE-2026-18556: N-central 2026.1 and all earlier versions
- CVE-2026-18577: N-central 2026.3.1 and all earlier versions, prior to Hotfix 1, that is all builds earlier than 2026.3.1.7

Solution for both issues: upgrade to N-central 2026.3 Hotfix 1 (build 2026.3.1.7) or above.

Both vendor-hosted (cloud) and on-premises (self-hosted) deployments are affected.

What does this mean?

Background - how these vulnerabilities are being exploited:

- An attacker reaches an N-central server over the network. No credentials, phishing or brute-force activity are required beforehand.
- Authentication controls are bypassed through an alternate path or channel, granting the attacker the same level of access as a platform administrator. N-able has not published root-cause detail, and neither CVE record identifies the vulnerable endpoint or request sequence.

Mitigation process

CERTVU recommends the following:

- Upgrade all N-central servers to 2026.3 Hotfix 1 (build 2026.3.1.7) or above without delay, then upgrade N-central agents on managed endpoints.
- Restrict access to the N-central management interface to trusted administrative networks, and enforce multi-factor authentication on all administrative accounts.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-18556
2. https://www.cve.org/CVERecord?id=CVE-2026-18577
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
4. https://www.n-able.com/blog/n-central-security-update-august-2-2026
5. https://status.n-able.com/2026/08/02/n-central-2026-3-hotfix-1-mitigation-for-cve-2026-18577/
6. https://cwe.mitre.org/data/definitions/288.html