Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

N-able Confirms Active Exploitation of N-central Authentication Bypass Flaw

Date of Publication	Last Update Date	Admiralty Code	TA Number
August 04, 2026	August 10, 2026	A1	TA2026219

Summary

First Seen: July 31, 2026
Affected Products: N-able N-central
Impact: CVE-2026-18577 is an authentication bypass vulnerability in N-central, N-able's flagship remote monitoring and management platform used by managed service providers and enterprise IT teams to oversee servers, workstations, and network devices across their client base. The flaw results from an incomplete fix for an earlier authentication bypass issue, CVE-2026-18556, and allows an unauthenticated attacker to gain full administrative access to the N-central console on both cloud-hosted and self-hosted deployments running any version through 2026.3. Attackers have been observed abusing this access through the platform's built-in Take Control feature to pivot into managed endpoints, including domain controllers, and to establish persistence through Cloudflare tunnels disguised as a legitimate-looking service. Active exploitation was detected on August 1, 2026, and a hotfix was released the following day to close the gap. No specific threat actor has been publicly attributed to the activity, and unpatched self-hosted servers remain the primary source of continued risk.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-18577	N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability	N-able N-central	✗	✓	✓
CVE-2026-18556	N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability	N-able N-central	✗	✓	✓

Vulnerability Details

#1

Attackers are exploiting an authentication bypass vulnerability (CVE-2026-18577) in N-able N-central, a remote monitoring and management (RMM) solution widely used by managed service providers, to gain access to managed endpoints. N-able first noticed anomalous activity on July 31, 2026, confirmed active exploitation the next day, and released an emergency hotfix on August 2.

#2

The flaw is an authentication bypass using an alternate path or channel, tracked under CWE-288. It exists because an earlier fix for a related bypass, CVE-2026-18556, did not fully close that path, so attackers can still reach privileged functionality without a valid login. The issue affects every N-central version through 2026.3, on both cloud-hosted and self-hosted servers. Hosted customers were patched automatically, but self-hosted servers need manual updates, and many remained unpatched even after the fix was made public.

#3

Once inside a console, attackers gain the same access as a platform administrator. Observed activity includes checking running processes on compromised hosts, using N-central's built-in Take Control feature to reach into managed endpoints such as domain controllers, and setting up outbound tunnels disguised as a legitimate service to keep access open without needing an inbound firewall rule.

#4

The flaw reflects easy remote exploitation and serious impact to data confidentiality. Multiple independent sources confirm exploitation in the wild, including reconnaissance against domain controllers and fast movement across compromised networks. N-able has released a new round of hotfixes for N-central as part of its ongoing investigation into this exploitation. This update is not a repeat of the earlier notice. Hotfix 2 must be installed even if Hotfix 1 was already applied. Hotfix 2 replaces Hotfix 1 and adds extra security hardening to better protect partners and their customers. All partners are strongly urged to upgrade to this hotfix as soon as possible.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-18577	N-able N-central (Before 2026.3.1.7)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-288
CVE-2026-18556	N-able N-central (Before 2026.2)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-288

Recommendations

Apply the Hotfix Immediately: Upgrade every self-hosted N-central instance to build 2026.3.1.10, without delay. Hosted (NCOD) customers receive this update automatically, but on-premises deployments must install it manually to close the authentication bypass.

Hunt for Signs of Compromise: Check user Documents folders across managed devices for a file named svchost.exe and review the Windows services list for one registered as Cloudflared. Either finding should be treated as a likely incident, warranting immediate escalation to vendor support and the internal security team.

Restrict Console Exposure Until Patched: If the hotfix cannot be applied immediately, take the N-central console offline or restrict access to trusted administrative IP ranges through firewall rules or VPN. Avoid exposing the login page directly to the public internet in the interim.

Review Remote-Control and Login Activity: Audit recent Take Control sessions and console logins for connections from unfamiliar IP ranges, activity at unusual hours, or sessions touching domain controllers and other high-value systems without a matching support ticket.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Discovery	T1057: Process Discovery	
	T1018: Remote System Discovery	
Lateral Movement	T1219: Remote Access Software	
Command and Control	T1572: Protocol Tunneling	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	173[.]249[.]252[.]200, 87[.]249[.]138[.]34, 37[.]19[.]210[.]32, 68[.]235[.]46[.]214, 37[.]153[.]90[.]88, 92[.]118[.]112[.]181, 173[.]249[.]252[.]200, 185[.]156[.]46[.]150, 23[.]234[.]94[.]43, 68[.]235[.]46[.]235, 87[.]249[.]138[.]34
Domains	mousears[.]synology[.]me, wagoosh[.]direct[.]quickconnect[.]to, who-ripped-one[.]direct[.]quickconnect[.]to

Patch Link

https://status.n-able.com/2026/08/06/n-central-2026-3-hotfix-2-additional-mitigation-for-cve-2026-18577/

References

https://status.n-able.com/2026/08/02/n-central-2026-3-hotfix-1-mitigation-for-cve-2026-18577/

https://www.n-able.com/blog/n-central-security-update-august-2-2026

https://www.n-able.com/blog/n-central-security-update-august-6-2026

https://status.n-able.com/2026/08/06/n-central-2026-3-hotfix-2-additional-mitigation-for-cve-2026-18577/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

August 04, 2026 • 11:00 AM

More at www.hivepro.com