Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# N-able N-central Pre-Auth RCE Exploited in the Wild (CVE-2026-86218)


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| September 10, 2026 | A1 | TA2026265 |

# Summary

**First Seen:** September 4, 2026
**Affected Products:** N-able N-central
**Impact:** N-able has patched a maximum-severity flaw in N-central, the remote monitoring and management (RMM) platform that managed service providers and IT teams rely on to run thousands of client devices from a single console. Tracked as CVE-2026-86218 and carrying the worst-possible CVSS score of 10.0, the bug is a static code injection weakness that lets an attacker run their own code on an N-central server without ever logging in. N-able shipped an emergency fix, N-central 2026.3 Hotfix 4, on September 5, 2026, and CISA added the flaw to its Known Exploited Vulnerabilities catalog days later, ordering federal agencies to patch by September 11. No specific threat actor or malware family has been publicly tied to the activity yet, but scanning and exploitation attempts were already underway before the patch landed.

## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-86218 | N-able N-central Static Code Injection Vulnerability | N-able N-central | ✓ | ✓ | ✓ |

# Vulnerability Details

**#1**

CVE-2026-86218 is a critical zero-day code injection vulnerability in N-able N-central, the web-based console MSPs and large IT organizations use to monitor and manage client networks. The flaw stems from the server accepting attacker-controlled input and treating it as executable code rather than inert data. The practical result is pre-authentication remote code execution: an attacker can run commands on the N-central server before any login or authentication step, which is what pushes the severity to the maximum.

**#2**

The vulnerability is exploitable remotely against internet-facing N-central instances in low-complexity attacks that require no privileges and no user interaction. Because N-central is designed to reach down into every device and customer environment it manages, code executed on the server does not stay contained to the appliance; changes made through a compromised N-central can propagate across all connected systems, which is exactly why the platform is so attractive to ransomware operators.

**#3**

The issue affects N-central builds before 2026.3.1.14, delivered as N-central 2026.3 Hotfix 4. Deployments still running the earlier Hotfix 3 remain exposed to this specific flaw, so HF3 is not a sufficient fix. Both hosted and on-premises deployments were listed as impacted; N-able patched hosted environments server-side, while on-premises operators must apply the update themselves.

**#4**

CVE-2026-86218 carries a CVSS score of 10.0, while N-able's own urgent customer notice stated the flaw had been observed being exploited in the wild. The flaw was exploited before a patch was available. The disclosure landed on the heels of two related authentication-bypass flaws in N-central, CVE-2026-86206 and CVE-2026-86207 (patched in Hotfix 3), which can be chained to create an attacker-controlled administrator account; investigators were unable to confirm which flaw was used in an early September intrusion because logs on the compromised appliance had already rotated.

# Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2026-86218 | N-able N-central (Before 2026.3.1.14) | cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:* | CWE-96 |

# Recommendations

**Apply Hotfix 4 Without Delay:** Upgrade every on-premises N-central deployment to 2026.3 Hotfix 4 (build 2026.3.1.14), which closes this vulnerability. Deployments still on Hotfix 3 are not protected against this flaw, so treat HF4 as mandatory rather than optional. Hosted N-central environments were already patched server-side by N-able and need no customer action.

**Reduce Internet Exposure:** Where possible, avoid exposing the N-central management console directly to the open internet. Place it behind a VPN, restrict access to a trusted IP allowlist, and ensure administrative interfaces are reachable only from known networks. Limiting who can reach the server shrinks the attack surface for this flaw and future ones.

**Vulnerability Management:** Maintain an accurate inventory of software versions and applied patches, and monitor vendor advisories so emergency hotfixes like this one are applied quickly. Give particular scrutiny to RMM and other management tooling that sits above your wider environment, since a single weakness in these platforms can cascade across every connected system and vendor relationship.

**Hunt for Signs of Compromise:** Review your logs for scanning or connection attempts from the IP range 23.234.64.0/18, which N-able observed probing for this vulnerability. Audit your N-central deployment for unfamiliar or newly created user accounts, especially any unexpected administrator-level accounts, and investigate anything you cannot account for. Because appliance logs rotate quickly, prioritize this review even if a system was patched promptly.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1190: Exploit Public-Facing Application | |
| Execution | T1059: Command and Scripting Interpreter | |
| Resource Development | T1588: Obtain Capabilities | T1588.006: Vulnerabilities |

## Patch Links

https://www.n-able.com/blog/n-central-security-hotfix-september-5-2026

https://status.n-able.com/2026/09/06/n-central-2026-3-hotfix-4-cve-2026-86218/

## References

https://me.n-able.com/s/security-advisory/aArVy0000002Ld3KAE/cve202686218-preauthentication-remote-code-execution

https://documentation.n-able.com/N-central/Release_Notes/GA/Content/N-central_2026.3_HF4_Release_Notes.htm

# 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

**September 10, 2026 • 08:30 AM**

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com