N-able releases hotfixes for publicly disclosed N-central zero-days



N-able released N-central 2026.4 HF2 to fix several publicly disclosed zero-day flaws and urges on-premises customers to upgrade quickly. A threat intelligence firm reports scanning for the flaws.

- N-central 2026.4 HF2 patches several of the leaked zero-days, including those N-able calls the most critical.
- N-able says all hosted N-central servers have been upgraded; on-premises customers are strongly urged to upgrade as soon as possible.
- Defused reports probing activity, including anonymous agent sessions and unauthenticated access to the remote control endpoint.
- Shadowserver counts just over 148 exposed N-central servers, down from 1,338 on Monday.

> - N-able has not yet flagged the flaws as exploited in the wild.

N-able has released N-central 2026.4 HF2, a hotfix for zero-day vulnerabilities in its N-central remote monitoring and management platform. The flaws were published by an independent researcher on November 8, and N-able took its hosted environments offline as a precaution while it prepared fixes.

What was fixed

The hotfix addresses several of the disclosed issues, including those N-able describes as the most critical. They include XXE and OGNL injection flaws (CVE-2026-125883, CVE-2026-125878), local privilege escalation (CVE-2026-125879, CVE-2026-91000), stored XSS (CVE-2026-125880), SSRF (CVE-2026-125881) and remote code execution through a file upload path traversal (CVE-2026-125882).

The researcher also demonstrated an unauthenticated chain that could let an attacker run commands on the server and create a rogue Default Administrator account. N-able says the hosted servers are now upgraded. It strongly recommends that on-premises customers upgrade as soon as possible and follow its published guidance before restoring normal access.

Current exposure

N-able has not yet marked the flaws as exploited. However, Defused reports probing over the past 24 hours, including anonymous agent sessions, appliance configuration retrieval and unauthenticated requests to the remote control endpoint. Shadowserver sees just over 148 exposed servers, down from 1,338 on Monday.

Because N-central manages client networks and devices from one console, organizations that run it themselves, or rely on a provider that does, should treat this as a priority change.

What to do now

1. Identify whether N-central is used internally or by any managed service provider with access to your environment.
2. Upgrade on-premises N-central to 2026.4 HF2 following N-able's published guidance before restoring access.
3. Ensure N-central servers are not reachable from the internet; restrict management access to trusted networks or VPN.
4. Review N-central logs for anonymous agent sessions, unexpected Default Administrator accounts and unauthenticated remote control requests.
5. Reset N-central administrator credentials and review accounts if suspicious activity is found.
6. Ask your MSPs to confirm their patch status and report any suspected compromise.