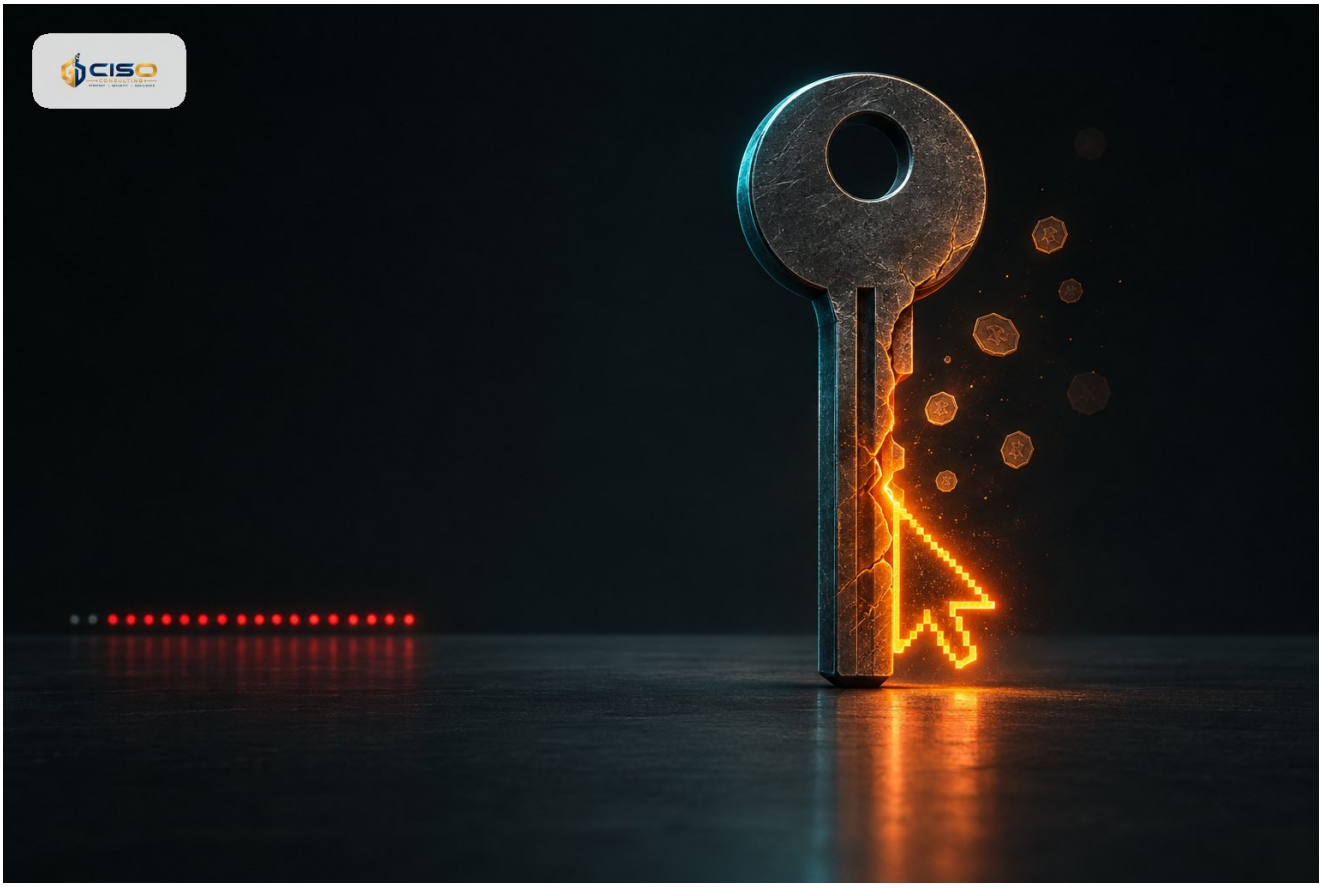
N-able N-central "4EverAble2Shell" zero-day exploited within hours of public PoC



Attackers are exploiting a new N-central zero-day, 4EverAble2Shell, to gain root access and install crypto miners. Researchers confirmed 21 compromised servers, 19 of them on the latest hotfix.

- 4EverAble2Shell lets unauthenticated attackers run commands as root on N-central servers when Legacy API is enabled.
- The chain combines Apache Axis CVE-2026-90436 with a separate N-central privilege escalation flaw.
- Huntback confirmed 21 compromised hosted N-central servers, 19 on version 2026.4.1.26 (Hotfix 2).
- Observed payloads install an XMRig Monero miner, but compromised RMM servers could be used

against managed customers.

- N-able disabled the Intune integration and urges on-premises customers to keep Legacy API disabled.

What happened

A researcher, Sean Bales, published proof-of-concept code for two new N-central zero-days, 4EverAble2Shell and Agent2Shell. Exploitation of 4EverAble2Shell began on November 12, shortly after release. N-central is a remote monitoring and management (RMM) platform used by managed service providers and IT teams.

The 4EverAble2Shell chain lets an unauthenticated attacker run commands as root, provided the Legacy API is enabled. It uses Apache Axis CVE-2026-90436 to run commands as the service account, then a separate privilege escalation flaw to reach root. Agent2Shell is claimed to give SYSTEM-level command execution on Windows devices.

Observed exploitation

Previdian and Huntback both saw probing of honeypots at about 08:30 UTC, followed by attempts to run the full chain. Huntback found 21 hosted N-central servers running attacker miners, 19 of them on version 2026.4.1.26, the Hotfix 2 release of November 10. The payload installed an XMRig Monero miner set to use about half the CPU cores.

The attacks so far are cryptojacking, but root access to an RMM server could enable further activity against managed customer environments.

Vendor response

N-able is restricting some features and integrations, has disabled the Intune integration, and asks on-premises customers to confirm Legacy API is disabled, which is the default. It also advises continuing to upgrade Agents and Probes under the Hotfix 2 guidance. Its advisory said it had seen no compromise from the new flaws, though researchers have since reported successful attacks.

What to do now

1. Identify all N-central instances, including those run by MSPs on your behalf, and confirm Legacy API is disabled.
2. Search web logs for requests to /dms/services/ServerUI, especially those referencing jline.internal.TerminalLineSettings.
3. Hunt for unexpected xvd.service systemd services, mining processes, and files under /tmp/.xvd or /var/tmp/.xvd.
4. Treat any server showing these indicators as fully compromised, and review managed endpoints and

credentials it could reach.

5. Ask your MSPs in writing about their exposure and compensating controls, and keep Agents and Probes updated per N-able guidance.