N-able Releases N-central 2026.4 Hotfix 3 as Earlier Flaws Are Exploited



N-able has issued N-central 2026.4 Hotfix 3, a critical security update for its RMM and UEM platform. The headline reports 17 flaws fixed and attackers exploiting earlier bugs to deploy crypto miners.

- N-able released N-central 2026.4 Hotfix 3 and describes it as a critical security update.
- The headline says the update fixes 17 flaws in N-central.
- N-central is a Remote Monitoring and Management (RMM) and Unified Endpoint Management (UEM) platform.
- The headline reports attackers exploiting earlier bugs to deploy crypto miners.
- The available excerpt does not give CVE numbers or technical details.

What happened

N-able has released N-central 2026.4 Hotfix 3, which the company describes as a critical security update. It contains security patches and fixes intended to strengthen the N-central platform, used for Remote Monitoring and Management (RMM) and Unified Endpoint Management (UEM). According to the source headline, the update addresses 17 flaws.

The same headline reports that attackers have exploited earlier bugs in the product to deploy crypto miners. The excerpt we reviewed is partial, so it does not list CVE identifiers, affected version ranges beyond the 2026.4 release line, or details of the attacks.

Why it matters

RMM and UEM platforms hold privileged access to many endpoints at once. A weakness in such a tool can give an attacker a route into every device it manages, which is why a vendor-labelled critical update deserves prompt attention. Organisations that rely on N-central directly, or through a managed service provider, should treat this as a priority review.

What to do next

Confirm whether N-central is in use in your environment, including by your service providers, and check the vendor's release notes for the full list of fixes. Apply the hotfix through your normal emergency change process, and look for signs of unexpected software or abnormal resource use on managed endpoints.

What to do now

1. Identify all N-central instances in your estate, including those run by managed service providers.
2. Review N-able's release notes for Hotfix 3 and apply it through your emergency change process.
3. Hunt for unexpected processes or unusual CPU usage on endpoints managed by N-central.
4. Review administrator accounts and access to the N-central console, and restrict exposure where possible.
5. Ask service providers to confirm in writing their patch status and any signs of compromise.