CISA flags exploited N-able Mail Assure flaw as the vendor restores service



CISA added CVE-2026-134624, a 9.3-rated flaw in N-able Mail Assure, to its exploited vulnerabilities catalogue. N-able says it has remediated the issue and found exploitation only on one of its own servers.

- CVE-2026-134624 affects N-able's Mail Assure email security platform and carries a 9.3 severity score.
- CISA added it to its exploited vulnerabilities list and set a Thanksgiving deadline for U.S. federal agencies.
- Attackers breached one N-able-hosted server through the bug, disrupting Mail Assure and SpamExperts services for about a week.
- N-able says mail flow and spam filtering kept running, and it found no exploitation beyond that

> single server.
>
> - A root cause analysis is promised within two weeks; the company says this is unrelated to the recent N-central vulnerabilities.

CISA has added CVE-2026-134624, a vulnerability in N-able's Mail Assure email security platform, to its catalogue of exploited vulnerabilities. The flaw has a severity score of 9.3, and U.S. federal agencies have been told to patch it by Thanksgiving.

What happened

According to the report, attackers used the bug to breach one N-able-hosted server, which led to roughly a week of outages affecting Mail Assure and SpamExperts services. N-able told Recorded Future News that it remediated the flaw over the weekend and restored customer access to internal dashboards. It says inbound and outbound email and spam filtering kept working throughout.

The company reports that continued scanning and monitoring found no exploitation beyond the single server identified at the start, and that it engaged incident responders to validate this. It has promised a root cause analysis within two weeks.

Related N-able issues

N-able says this incident is not connected to more than 30 vulnerabilities in its N-central remote management platform, which a researcher disclosed two weeks earlier. For those, N-able took hosted N-central environments offline and told customers to shut down their servers. The report also notes that an N-central bug featured in a ransomware supply-chain attack in August.

Why it matters

Email security services and remote management tools sit in a privileged position in an organisation's environment. Institutions that use N-able products directly, or through a managed service provider, should confirm their exposure and ask for written assurance rather than rely on public statements alone.

What to do now

1. Identify whether Mail Assure, SpamExperts or N-central is used in your environment, including through managed service providers.
2. Request written confirmation from N-able or your provider on remediation status and whether your tenant was affected.
3. Review mail gateway and administrative logs for unusual activity and unexpected configuration changes.
4. Rotate credentials and API keys tied to the affected services if your provider cannot rule out exposure.

5. Track the promised root cause analysis and update your third-party risk assessment accordingly.
6. Follow your incident reporting obligations to the relevant regulator if you confirm impact.