# N-able patches critical SSRF flaw found during Mail Assure incident investigation



N-able patched CVE-2026-134624 (CVSS 9.3), an SSRF flaw found while investigating the cyberattack on Mail Assure and SpamExperts. Customers should confirm they run the fixed version and review credentials.

- CVE-2026-134624 is an SSRF flaw rated CVSS 9.3, fixed in Mail Assure/SpamExperts version 20261121.1943.
- The flaw lets a sufficiently privileged API user make the server connect to arbitrary internal hosts and ports and send crafted data.
- The earlier attack hit a web server and likely exposed stored credentials; N-able rotated credentials and revoked API and OAuth tokens.
- N-able says exploitation was confined to one N-able-hosted server and further monitoring found

no malicious activity.

- A formal root cause analysis is promised within two weeks.

N-able has patched a critical server-side request forgery (SSRF) vulnerability, tracked as CVE-2026-134624 with a CVSS score of 9.3. The flaw was found during the company's investigation into a cyberattack on its Mail Assure and SpamExperts Hosted Cloud services.

## What happened

On November 16, N-able disabled access to the portal and API and suspended related services, including logging, mailbox synchronization, the management portal and quarantine. Email delivery was not affected. The company later confirmed a cyberattack in which the attackers hit a web server and likely accessed certain credentials stored on it.

N-able contained the incident, changed credentials and revoked API and OAuth tokens. Access to the dashboard and APIs was restored on November 21 under continued monitoring.

## The vulnerability

The service did not restrict the destination of the LDAP synchronization connection check performed when a relay is configured. An API user with sufficient privileges could therefore make the server connect to arbitrary internal hosts and ports, identify which are reachable, and send crafted data to internal services. Version 20261121.1943 contains the fix.

N-able states that exploitation was confined to a single N-able-hosted server and that monitoring since remediation has shown no further malicious activity. Its investigation continues, and a formal root cause analysis is expected within two weeks.

## Why it matters

Organizations that use these services for email filtering should treat this as a supplier incident: confirm their own exposure, check credentials and tokens tied to the service, and track the forthcoming root cause analysis.

## What to do now

1. Confirm with N-able whether your tenant runs Mail Assure/SpamExperts version 20261121.1943 or later.
2. Rotate any credentials, API keys and OAuth tokens associated with the service, even if N-able has already revoked its own.
3. Review which users hold API privileges on the service and remove those that are not needed.
4. Check logs for unusual API or LDAP synchronization activity and for unexpected internal connections from the service.

5. Log the event under your third-party incident process and request the root cause analysis from N-able when published.