N-able Discloses Critical SSRF Flaw in Mail Assure, Found During Breach Investigation



N-able disclosed CVE-2026-134624, a critical SSRF flaw in its Mail Assure and SpamExperts Hosted Cloud email filtering service, found while investigating a breach of that service.

- The flaw is tracked as CVE-2026-134624 and rated critical.
- It is a server-side request forgery (SSRF) issue in Mail Assure and SpamExperts Hosted Cloud.
- A user with high-level API access could open connections to internal systems of their choosing.
- N-able found it while investigating a breach of the same hosted email filtering service.
- The service is run for managed service providers.

N-able has disclosed a critical vulnerability in Mail Assure and SpamExperts Hosted Cloud, the email filtering

service it operates for managed service providers (MSPs). The company found the flaw while investigating a breach of that service.

What was disclosed

The issue is tracked as **CVE-2026-134624** and is a server-side request forgery (SSRF) vulnerability. According to the report, a user with high-level API access could make the service open connections to internal systems of the user's choosing.

The excerpt available to us does not describe the full scope of the breach, the affected versions, any patch or mitigation details, or whether customer data was accessed. We have not filled those gaps and recommend reading N-able's own advisory for them.

Why it matters for Saudi institutions

Institutions that receive email filtering through an MSP may depend on this service without a direct contract with N-able. An SSRF flaw in a hosted platform is a supplier-side risk: the exposure sits in the provider's environment, so the institution's visibility depends on what the provider tells it.

Recommended approach

Treat this as a third-party risk question first. Establish whether you or your MSPs use the service, ask for the provider's written assessment, and review your own exposure while details are confirmed.

What to do now

1. Check with your MSPs and email security vendors whether Mail Assure or SpamExperts Hosted Cloud is part of your mail flow.
2. Read N-able's official advisory for CVE-2026-134624 and confirm affected components and any required customer steps.
3. Ask the provider in writing whether your tenant or data was affected by the breach and what was done about it.
4. Review API keys and high-privilege accounts tied to the service, and rotate or restrict them where appropriate.
5. Log the issue in your third-party risk register and follow the incident notification terms in your contracts.