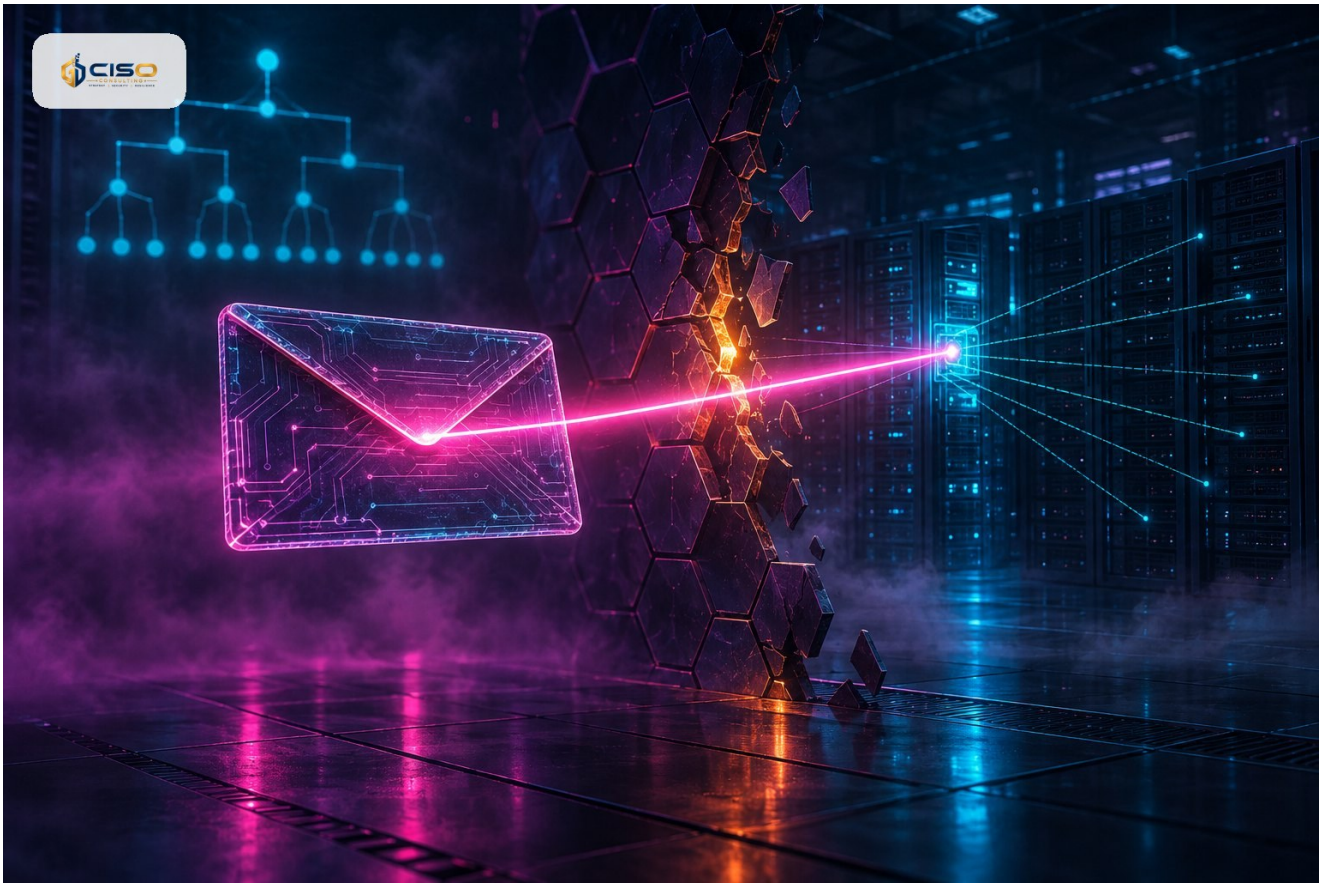
N-able MailAssure SSRF flaw (CVE-2026-134624): apply vendor mitigations



CISA lists CVE-2026-134624, an SSRF flaw in the LDAP synchronization check of N-able MailAssure (SpamExperts). An authenticated API user could probe internal hosts and ports and send crafted data to internal services.

- The flaw is a server-side request forgery in the LDAP synchronization connection check of N-able MailAssure (SpamExperts).
- An authenticated API user can reach arbitrary internal hosts and ports and learn which are reachable.
- The same user can send crafted data to internal services.
- CISA requires mitigations per vendor instructions, in line with BOD 26-04 and its forensics triage requirements.

> - If mitigations are unavailable, CISA says to discontinue use of the product; the federal due date is 2026-11-26.

CISA has added CVE-2026-134624 to its catalogue. It is a server-side request forgery (SSRF) vulnerability in N-able MailAssure (SpamExperts), located in the connection check used for LDAP synchronization.

What the flaw allows

An authenticated API user can make the product connect to arbitrary internal hosts and ports. By doing so, the user can work out which internal systems are reachable and can send crafted data to internal services. The source does not describe any specific exploitation or affected versions.

What CISA requires

CISA's required action is to apply mitigations according to the vendor's instructions, consistent with its BOD 26-04 guidance on prioritizing security updates based on risk and its forensics triage requirements. Where mitigations are not available, the guidance is to follow the BOD 26-04 provisions for cloud services or stop using the product. Stakeholders are expected to assess each asset's internet exposure themselves. The federal due date is 2026-11-26.

Relevance for Saudi institutions

BOD 26-04 binds US federal agencies, but the same discipline suits regulated institutions in the Kingdom that run MailAssure. Because exploitation needs an authenticated API user, access to the API and the credentials that unlock it deserve attention alongside patching.

What to do now

1. Identify whether N-able MailAssure (SpamExperts) is used in your environment, including via managed or cloud services.
2. Apply the vendor's mitigations and record the date and scope of the change.
3. Review who holds API credentials, remove unneeded accounts and rotate the credentials of those that remain.
4. Check API and server logs for LDAP synchronization connection checks aimed at unexpected internal hosts or ports.
5. Where mitigations are unavailable, plan to discontinue the product, as CISA advises, and note the decision in your risk register.