CISA adds N-able MailAssure and MONAI Label flaws to its exploited-vulnerabilities list



CISA has added two critical flaws, in N-able MailAssure and MONAI Label, to its Known Exploited Vulnerabilities catalog, citing evidence of active exploitation. The MailAssure flaw is an SSRF issue with a CVSS score of 9.3.

- CISA added the two vulnerabilities to its KEV catalog on Monday, citing evidence of active exploitation.
- The flaws affect N-able MailAssure and MONAI Label and are described as critical.
- CVE-2026-134624 is a server-side request forgery (SSRF) flaw in N-able MailAssure's LDAP component, with a CVSS score of 9.3.
- The source excerpt available to us does not give full details of the MONAI Label flaw.

What happened

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added two critical vulnerabilities, affecting N-able MailAssure and MONAI Label, to its Known Exploited Vulnerabilities (KEV) catalog. The agency cited evidence of active exploitation.

One of them, **CVE-2026-134624**, is a server-side request forgery (SSRF) vulnerability in the LDAP functionality of N-able MailAssure. It carries a CVSS score of 9.3.

What we do not yet know

The excerpt of the report available to us is truncated. It does not set out the technical details of the MONAI Label flaw, the affected versions, or any vendor fix. Readers should consult the CISA KEV entries and the vendors' own advisories before acting on specifics.

Why it matters

Inclusion in the KEV catalog signals that exploitation is happening in practice, not only in theory. Organisations that run MailAssure, an email security service, or MONAI Label should treat these as priority items and verify their exposure rather than wait for a routine patch cycle.

What to do now

1. Check whether MailAssure or MONAI Label is deployed anywhere in your estate, including by third-party providers.
2. Read the CISA KEV entries and the vendor advisories for affected versions and fixes.
3. Apply vendor patches or mitigations on a priority basis once confirmed.
4. Review logs of affected systems for unusual outbound or internal requests, which may point to SSRF abuse.
5. Record the exposure and remediation in your vulnerability management process under NCA ECC and SAMA CSF requirements.