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



CISA has added two vulnerabilities to its KEV Catalog on evidence of active exploitation: a path traversal flaw in MONAI Label and an SSRF flaw in N-able Mail Assure (SpamExperts). Check whether you run either product.

- CVE-2026-133968 is a path traversal vulnerability in Project MONAI MONAI Label.
- CVE-2026-134624 is a server-side request forgery (SSRF) vulnerability in N-able Mail Assure (SpamExperts).
- Both were added to the KEV Catalog based on evidence of active exploitation.
- CISA describes these vulnerability types as a frequent attack vector for malicious actors.
- BOD 26-04 binds only US federal civilian agencies, but CISA encourages all organizations to prioritize KEV-listed flaws.

CISA has added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog after finding evidence that they are being exploited in the wild.

What was added

- **CVE-2026-133968**: a path traversal vulnerability in Project MONAI's MONAI Label.
- **CVE-2026-134624**: a server-side request forgery (SSRF) vulnerability in N-able Mail Assure (SpamExperts).

CISA notes that vulnerabilities of these types are a frequent attack vector for malicious cyber actors. The source does not give affected versions, patch details or information about who is exploiting the flaws, so consult the vendors' own advisories for that.

Why it matters beyond the US

Binding Operational Directive 26-04 requires US Federal Civilian Executive Branch agencies to fix KEV-listed vulnerabilities quickly, particularly on publicly exposed assets where exploitation gives full control. It also sets expectations for checking whether a system was compromised before a patch was applied. The directive does not apply to organizations outside those agencies, yet CISA encourages all organizations to adopt risk-based vulnerability management and to prioritize KEV Catalog entries.

For Saudi institutions, the practical step is modest: confirm whether either product is in your estate, including in the hands of managed service providers, and treat a match as a priority item in your patching queue.

Next steps

Use the actions below to confirm exposure, apply vendor fixes and look for signs of earlier compromise.

What to do now

1. Search your asset inventory and service-provider contracts for MONAI Label and N-able Mail Assure (SpamExperts).
2. Review the vendors' advisories and apply available fixes or mitigations, starting with internet-facing instances.
3. Check logs and systems for signs of compromise that predate patching.
4. Add KEV Catalog entries to your vulnerability-management triage as a high-priority input.
5. Ask managed service providers to confirm whether they use either product on your behalf.