CISA KEV roundup: MONAI Label path traversal and N-able Mail Assure SSRF (CVE-2026-133968, CVE-2026-134624)

Status: Recovering / monitoring

Started Nov 28, 2026, 11:36 AM PST · Project MONAI; N-able's estimate: Fixed versions are available

CVE-2026-133968, CVE-2026-134624 · Being exploited: yes · Fix available: yes

WHAT'S HAPPENING

CISA, the US government's cyber defense agency, keeps a list of security flaws that criminals are known to be using. On November 23, 2026 it added two. CVE-2026-133968 is a 'path traversal' flaw in MONAI Label. <cite index="2-5">It could let an unauthenticated remote attacker write files outside the intended folder, potentially leading to remote code execution (running the attacker's own commands).</cite> The CVSS severity score is 9.8 out of 10. CVE-2026-134624 is a 'server-side request forgery' (SSRF) flaw in N-able Mail Assure. <cite index="2-4">It lets an authenticated API user connect to internal hosts and ports, check which are reachable, and send crafted data to internal services.</cite> It is scored 9.3. <cite index="3-7">N-able disclosed a security incident that disrupted Mail Assure and SpamExperts Hosted Cloud on November 16, 2026.</cite> <cite index="3-8">An N-able spokesperson said the company remediated the incident and restored the affected functions.</cite> <cite index="2-6">US federal civilian agencies were told to apply fixes by November 26, 2026.</cite>

WHO IS AFFECTED

- MONAI Label 0.8.5 and earlier (fixed in 0.8.6), mainly self-hosted servers used in medical imaging and research
- N-able Mail Assure and SpamExperts builds earlier than 20261121.1943. The Hosted Cloud service is patched centrally by N-able; customers running a Local Cloud (their own hardware) must update themselves.
- Ordinary home users are unlikely to run either product directly. Your risk comes mainly through an organization that does, such as an IT provider that uses Mail Assure to filter email.

IS IT BEING EXPLOITED?

CISA added both flaws to its Known Exploited Vulnerabilities (KEV) catalog on Monday, November 23, 2026, citing evidence of active exploitation. CISA lists known ransomware use for both as unknown. Reporting says the MONAI Label flaw was exploited in the wild from September 2026, before its public disclosure on November 20. For Mail Assure, N-able says it found no evidence of exploitation beyond a previously identified N-able-hosted server. N-able has not confirmed whether this flaw was the one used for initial access.

WHAT YOU SHOULD DO NOW

Home users

- You most likely don't run either product, so no action is needed on your own devices.
- If your employer, clinic, or IT provider uses N-able Mail Assure or MONAI Label, ask them whether the updates have been applied.
- Be careful with unexpected emails and password-reset requests as usual, and use multi-factor authentication where offered.

Businesses

- Find out whether you or your IT provider run MONAI Label or Mail Assure/SpamExperts, including Local Cloud installations.
- MONAI Label: upgrade to 0.8.6 or later. Don't expose the server directly to the internet; restrict access to trusted networks or a VPN.

• Mail Assure/SpamExperts Local Cloud: update to build 20261121.1943 or later. Hosted Cloud customers don't need to patch, but should confirm status with N-able.

• Mail Assure: one security write-up recommends rotating API and OAuth tokens (access credentials), and reviewing relay LDAP (directory) settings and outbound connections.

• Review logs for unusual activity, such as unexpected file creation on MONAI servers or odd internal connections from the mail filtering service. If you find signs of compromise, treat the system as breached and call your IT or incident response provider.

• Check N-able's own advisory and CISA's KEV entry for the latest guidance, because details are still emerging.

HOW TO CHECK IF YOU'RE AFFECTED

• MONAI Label: on the server, run 'pip show monailabel' in the Python environment that runs it, or check the version your deployment lists. Anything below 0.8.6 is affected.

• Mail Assure/SpamExperts Local Cloud: check the build number in the admin interface or ask your administrator. Anything before 20261121.1943 needs updating. The exact menu location isn't confirmed in the sources I reviewed, so check N-able's documentation.

• Hosted Cloud customers: no installed version to check. Confirm with N-able that the fix is in place.

FIXED VERSIONS AND WORKAROUNDS

• MONAI Label: 0.8.6

• N-able Mail Assure / SpamExperts: Build 20261121.1943

Until you can update:

• No official workarounds were confirmed in the sources I reviewed; updating is the recommended fix.

• Until you can update, limit network access to MONAI Label servers and to Mail Assure API access to trusted users and networks only.

OTHER COVERAGE

The Hacker News: Hackers Exploit N-able MailAssure Flaw While AI Agents Exploit MONAI Label Zero-Day — https://thehackernews.com/2026/11/hackers-exploit-n-able-mailassure-flaw.html

SecurityWeek: N-able Patches Critical Flaw Discovered After Mail Assure Cyberattack — https://www.securityweek.com/n-able-patches-critical-flaw-disclosed-after-mail-assure-cyberattack/

Security Affairs: U.S. CISA adds N-able MailAssure and Project MONAI flaws to its Known Exploited Vulnerabilities catalog — https://securityaffairs.com/203882/hacking/u-s-cisa-adds-n-able-mailassure-and-project-monai-flaws-to-its-known-exploited-vulnerabilities-catalog.html

ABOUT THIS BRIEF

Last updated November 28, 2026. Researched with AI help from public sources and checked against the official advisories above. Details can change; follow your vendor's guidance.

Questions? Contact BIS Computer Solutions, Inc.

5500 Alta Canyada Rd., La Canada, CA 91011 USA · Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com