CISA flags path traversal flaw in Project MONAI MONAI Label (CVE-2026-133968)



CISA lists CVE-2026-133968, a path traversal flaw in Project MONAI MONAI Label that lets an unauthenticated remote attacker write files outside the datastore directory, potentially leading to remote code execution.

- The flaw is a path traversal issue in Project MONAI MONAI Label.
- An unauthenticated remote attacker can write arbitrary files outside the intended datastore directory.
- Successful exploitation could result in remote code execution.
- CISA requires mitigations per vendor instructions, BOD 26-04 and its Forensics Triage Requirements.
- If no mitigation is available, CISA says to stop using the product; the federal due date is 2026-11-26.

CISA has added CVE-2026-133968 to its catalogue of vulnerabilities requiring action. The issue affects MONAI Label, part of Project MONAI, and is a path traversal weakness.

What the flaw allows

An unauthenticated attacker with network access can write arbitrary files outside the directory MONAI Label is meant to use as its datastore. Because the attacker can place files in locations the application should never touch, the flaw could lead to remote code execution on the affected system.

What CISA requires

CISA directs organisations to apply mitigations according to the vendor's instructions, in line with its BOD 26-04 guidance on prioritising security updates based on risk and its Forensics Triage Requirements. Where cloud services are involved, the applicable BOD 26-04 guidance should be followed. If mitigations are not available, CISA says use of the product should be discontinued. Stakeholders are expected to assess the internet exposure of each asset themselves. The federal due date is 2026-11-26; this deadline binds US federal agencies, but it is a useful benchmark for others.

Practical view

The source does not describe active exploitation details or affected versions, so teams should consult the vendor's instructions for scope and fixes. Institutions using MONAI Label, for example in medical imaging or research environments, should confirm where it runs and whether it can be reached from outside.

What to do now

1. Inventory every deployment of MONAI Label, including research and test environments.
2. Check whether each instance is reachable from the internet and restrict access until fixed.
3. Apply the vendor's mitigations; if none exist, plan to stop using the product.
4. Review affected hosts for unexpected files written outside the datastore directory and preserve evidence for forensic triage.
5. Record the vulnerability and remediation in the risk register and vulnerability management process.