AI Agents Used to Find Zero-Day in MONAI Label Medical Imaging Server



Amazon Threat Intelligence reports that suspected China-linked attackers used autonomous AI agents to find an unknown flaw in MONAI Label and gain root access to a university server. Versions 0.8.5 and earlier are affected in default setup.

- Suspected China-linked attackers used autonomous AI agents to discover a previously unknown flaw.
- The target was MONAI Label, an open-source medical imaging server.
- The flaw lets an unauthenticated attacker write files outside the server's storage folder.
- MONAI Label 0.8.5 and earlier are affected in the default configuration.
- The attackers gained root access to a university server, per Amazon Threat Intelligence.

Amazon Threat Intelligence said this week that suspected China-linked hackers used autonomous AI agents to find a previously unknown vulnerability in MONAI Label, an open-source server used for medical imaging work. The attackers then gained root access to a university server.

What is known

The flaw allows an attacker who has no account to write files outside the folder where the server keeps its data. It affects MONAI Label version 0.8.5 and earlier when run in its default setup. The source does not give a CVE number, a patch status or further technical detail, so those should be confirmed with the project's maintainers.

The notable point is the method: AI agents working autonomously were used to discover the weakness, not only to exploit it. This suggests that flaws in lesser-known open-source tools may be found faster than before.

Why it matters for healthcare and research

Hospitals, research centres and universities in the Kingdom may run imaging and AI tooling that sits outside the usual patient-system inventory. Such servers can hold sensitive data and are often reachable from internal networks, so a root-level compromise deserves attention even where the software is used only for research.

There is no need for alarm, but a short review is reasonable. Establish whether MONAI Label is in use, in which version, and who can reach it.

What to do now

1. Search asset inventories and research environments for MONAI Label and record the versions in use.
2. Restrict network access to any MONAI Label server so it is not reachable from untrusted networks.
3. Check the project's official channels for a fixed release or mitigation and apply it once confirmed.
4. Review server and file-write logs for unexpected files outside the storage folder.
5. Run such services with least privilege and isolate them from systems holding patient data.