AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-133968

Dateien schreiben ohne Anmeldung in MONAI Label (medizinische Bild-KI).

MONAI Label ist ein quelloffener Server, mit dem Kliniken und Forschungseinrichtungen medizinische Bilddaten mit KI-Unterstützung annotieren. Über den Upload-Endpunkt des Datenspeichers kann ein Angreifer aus dem Netz ohne Anmeldung Dateien an beliebige Stellen des Servers schreiben und so eigenen Code ausführen. Die Lücke wurde ab dem 08.09.2026 als Zero-Day gegen Universitäten ausgenutzt – gefunden von KI-Agenten eines Angreifers. Die Fixversion 0.8.6 ist seit dem 22.11.2026 verfügbar; die CISA führt die Lücke seit dem 23.11.2026 in ihrem KEV-Katalog.

> **Geschäftsrisiko:** Übernahme des Annotations-Servers mit Zugriff auf medizinische Bilddaten und Modelle, einem Brückenkopf ins Forschungs- oder Kliniknetz und einem möglicherweise meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO (Gesundheitsdaten nach Art. 9).

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Anmeldung, ohne Mitwirkung eines Nutzers, mit voller Wirkung auf das System. Basiswert laut CNA (MITRE), vom NVD übernommen; die eigene NIST-Bewertung steht noch aus.

AUSNUTZUNG BELEGT SEIT
08.09.2026 (laut Amazon Threat Intelligence)

BETROFFEN
MONAI Label bis 0.8.5 (Python-Paket monailabel)

HANDLUNGSBEDARF
Notfall-Change – sofort aktualisieren oder vom Netz nehmen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
PUT /datastore/image · Path Traversal (CWE-24)

Aktiv ausgenutzt
Zero-Day seit 08.09.2026 · CISA KEV seit 23.11.2026

0.8.6
Fixversion vom 22.11.2026

Die Ursache: Der Endpunkt `PUT /datastore/image` übernimmt den Abfrageparameter `image` ungeprüft als Bild-ID. Die Funktion `LocalDatastore.add_image()` hängt eine Dateiendung an, setzt den Pfad mit dem Datenspeicher-Verzeichnis zusammen und kopiert den Upload dorthin – **ohne zu prüfen, ob der Zielpfad im Datenspeicher bleibt (CWE-24, Path Traversal)**. Mit Sequenzen wie `../../` landet die Datei überall, wo der Serverprozess schreiben darf. Derselbe Fehler steckt in `PUT /datastore/label`. Die Authentifizierung ist in MONAI Label standardmäßig ausgeschaltet; ist sie aktiv, genügt die Rolle `ANNOTATOR`.

ANGRIFFSKETTE

01	02	03	04
Server erreichbar – MONAI Label antwortet aus dem Netz, Anmeldung standardmäßig aus	**Präparierter Upload** – PUT an /datastore/image mit ../-Sequenzen im Parameter image	**Datei platziert** – beobachtet: Reverse Shell in sitecustomize.py, die Python bei jedem Start lädt	**Code-Ausführung** – neuer Python-Prozess (z. B. Training) startet die Shell, im Fall als root

Betroffenheit & Fixversionen

MONAI-Label-Version	Verwundbar bis	Fixversion (Ziel)
MONAI Label bis 0.8.5	`alle Versionen < 0.8.6`	`0.8.6`
MONAI Label 0.8.6	nicht betroffen	—

Angaben laut GitHub Security Advisory GHSA-qc22-rmgc-vg94 und Release Notes 0.8.6 (22.11.2026). Version 0.8.6 schließt zusätzlich eine zweite Path-Traversal-Lücke beim Session-Upload (`PUT /session/?uncompress=true`). Die Release Notes empfehlen ausdrücklich, jeden Server bis 0.8.5, der aus nicht vertrauenswürdigen Netzen erreichbar war, auf unerwartete Dateiänderungen zu prüfen. **Das Einschalten der Anmeldung allein reicht nicht – die Rolle ANNOTATOR genügt für den Angriff.**

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf den Server kann eine meldepflichtige Verletzung darstellen – bei Gesundheitsdaten besonders sensibel; DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

08.–10.09.2026
Zero-Day-Ausnutzung gegen Universitäten in Ostasien (Amazon)

18.11.2026
GitHub Security Advisory GHSA-qc22-rmgc-vg94

20.–22.11.2026
CVE-2026-133968 · Amazon-Bericht · Release 0.8.6

23.11.2026
CISA KEV · Frist für US-Behörden 26.11.2026

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – vom Netz nehmen vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Erreichbarkeit einschränken	Update auf 0.8.6	Kompromittierung prüfen

01 Betroffenheit feststellen

Alle MONAI-Label-Server erfassen, auch Forschungs- und Laborinstallationen, Docker-Container und Plugins für 3D Slicer oder OHIF, die auf einen Server zeigen. Betroffen ist jede Version bis `0.8.5` (`pip show monailabel`). Klären, ob der Server aus dem Internet, aus Partner- oder Forschungsnetzen erreichbar ist.

02 Sofort Erreichbarkeit einschränken

Server aus nicht vertrauenswürdigen Netzen nehmen, Zugriff per Firewall oder VPN auf bekannte Nutzer begrenzen. Anmeldung einschalten (`MONAI_LABEL_AUTH_ENABLE=True`) und die Rolle `ANNOTATOR` nur vertrauenswürdigen Nutzern geben. Den Dienst als unprivilegierten Nutzer betreiben, der nur ins Datenspeicher-Verzeichnis schreiben darf.

03 Patchen

Auf `0.8.6` aktualisieren (`pip install -U monailabel` bzw. neues Docker-Image). Hinweis: 0.8.6 unterstützt Python 3.9 und 3.10 nicht mehr und nutzt im Image Ubuntu 24.04 mit Python 3.12 – Umgebung vorab prüfen.

04 Kompromittierung ausschließen

Webserver- bzw. Proxy-Logs auf PUT `/datastore/image` und `PUT /datastore/label` mit `../` oder URL-kodierten Varianten durchsuchen, mindestens zurück bis Anfang September 2026. Python-Installationen auf unerwartete `sitecustomize.py`- oder `.pth`-Dateien, geänderten Anwendungscode, SSH-Schlüssel und Cron-Einträge prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-IPS (08.–10.09.2026)

`142.4.98.145`
`142.4.107.34`

AUFFÄLLIGE DATEIEN

unerwartete `sitecustomize.py` im Python-Pfad
geänderte Anwendungsdateien, SSH-Keys, Cron

AUFFÄLLIGE MUSTER

PUT /datastore/image mit `../` im Parameter image
Shell- oder Netzwerkprozesse als Kind des Python-Prozesses

Zur Einordnung: Die IP-Adressen stammen aus dem Bericht von Amazon Threat Intelligence (Zeitraum 08. bis 10.09.2026) und sind eine Momentaufnahme. Die übrigen Muster sind Suchansätze aus dem dokumentierten Angriffsweg, kein vollständiger Ausschluss.

Wichtig: Die Lücke wurde von autonomen KI-Agenten in rund elf Minuten gefunden und ausgenutzt. Forschungs- und KI-Server laufen oft außerhalb des regulären Patchmanagements – genau dort setzen solche Werkzeuge an.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

Worauf wir bei dieser Schwachstelle achten: Ein MONAI-Label-Python-Prozess, der eine Shell oder ausgehende Verbindung startet. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Aus dem Netz erreichbare MONAI-Label-Server bis Version 0.8.5 über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre MONAI Label-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Update aller MONAI-Label-Server auf 0.8.6 als Notfall-Change anordnen.
- Bis dahin die Server aus offenen Netzen nehmen lassen.
- Eine Prüfung auf Kompromittierung seit September 2026 beauftragen.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-133968 und dem MONAI Label-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: GitHub Security Advisory GHSA-qc22-rmgc-vg94 (Project MONAI, 18.11.2026, betroffen bis 0.8.5, Fix 0.8.6) · MONAI Label Release 0.8.6 (22.11.2026) · NVD/CVE.org CVE-2026-133968 (CVSS 3.1 Basiswert 9,8 laut CNA, CWE-24, Ausnutzung ab September 2026) · Amazon Threat Intelligence, AWS Security Blog (20.11.2026, Kampagne ab 08.09.2026, IoCs) · CISA KEV (aufgenommen 23.11.2026, Frist 26.11.2026; SSVC: Ausnutzung aktiv, automatisierbar). Stand 23.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.