AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-10441

Codeausführung ohne Anmeldung auf Synology-NAS (DSM).

Ein Fehler im System-Plugin-Dienst von Synology DSM erlaubt es Angreifern, ohne Anmeldung aus dem Netz eigenen Code auf dem NAS auszuführen. Die Lücke ist seit November 2024 geschlossen, wird aber jetzt gegen veraltete Geräte ausgenutzt: Synology warnte am 29.10.2026 vor Ransomware-Angriffen, CISA führt die Lücke seit 18.11.2026 als aktiv ausgenutzt.

> **Geschäftsrisiko:** Verschlüsselung des Dateiservers samt der darauf liegenden Sicherungen – mit Betriebsunterbrechung, Lösegeldforderung und einem möglicherweise meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

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 NAS. Basiswert von Synology als CNA, von NVD übernommen.

AKTIV AUSGENUTZT
CISA KEV seit 18.11.2026

BETROFFEN
DSM 7.1, 7.2, 7.2.1, 7.2.2 vor den Fix-Builds
BeeStation OS vor 1.1-65374

HANDLUNGSBEDARF
Sofort – Ransomware-Angriffe laufen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
aus dem Netz · CWE-116

Aktiv ausgenutzt
CISA KEV seit 18.11.2026

Fix seit 2024
DSM-Update je Versionszweig

Die Ursache: Im **System-Plugin-Dienst** von DSM werden Ausgaben nicht korrekt kodiert bzw. maskiert (**CWE-116**). Laut Synology kann ein Angreifer darüber **ohne Anmeldung aus dem Netz beliebigen Code** ausführen; Details zum Angriffsweg nennt der Hersteller nicht. Die Lücke wurde beim Wettbewerb Pwn2Own 2024 gemeldet und im Advisory SA-24:20 geschlossen.

ANGRIFFSKETTE

01
NAS erreichbar – DSM-Dienste aus dem Internet oder dem Netz ansprechbar

02
Präparierte Anfrage – Angreifer spricht den System-Plugin-Dienst ohne Anmeldung an

03
Codeausführung – eigener Code läuft auf dem NAS

04
Verschlüsselung – Daten und lokale Sicherungen werden unbrauchbar gemacht

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
DSM 7.2.2	vor 7.2.2-72806-1	7.2.2-72806-1
DSM 7.2.1	vor 7.2.1-69057-6	7.2.1-69057-6
DSM 7.2	vor 7.2-64570-4	7.2-64570-4
DSM 7.1	vor 7.1.1-42962-7	7.1.1-42962-7
BeeStation OS	1.0, 1.1 vor 1.1-65374	1.1-65374

Laut Synology-Advisory SA-24:20 und CVE-Record. Der **vollständige Build-String inkl. Update-Nummer** entscheidet. Synology nennt keinen Workaround.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf ein NAS mit personenbezogenen Daten kann eine meldepflichtige Verletzung darstellen – 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

05.11.2024
Synology-Advisory + Fixes

19.03.2025
Veröffentlichung bei NVD

29.10.2026
Synology warnt vor Ransomware

18.11.2026
Aufnahme in CISA KEV

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Internetzugriff sperren	DSM aktualisieren	Auf Einbruch prüfen

01 Betroffenheit feststellen

Alle Synology-NAS und BeeStations erfassen, auch in Filialen und Abteilungen. Den vollständigen DSM-Build unter Systemsteuerung › Aktualisieren & Wiederherstellen mit Tabelle 1 abgleichen.

02 DSM aktualisieren

Auf den Fix-Build des eigenen Zweigs aktualisieren (z. B. `7.2.2-72806-1`) oder auf eine aktuelle DSM-Version. Auch die Pakete im Paket-Zentrum aktualisieren und automatische Updates einschalten.

03 Risiko bis zum Update senken

Die DSM-Verwaltung nicht direkt aus dem Internet erreichbar lassen: Portfreigaben am Router schließen, Fernzugriff nur über VPN. Sicherungen auf ein getrenntes Ziel außerhalb des NAS legen.

04 Kompromittierung ausschließen

Sicherheitsberater-Scan ausführen, im Aufgabenplaner nach fremden Skripten und unter Benutzer nach unbekannten Administratoren suchen. Dateien mit Endung `.L0CK3D` sind ein Alarmzeichen.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS	AUSWERTUNGSQUELLEN	AUFFÄLLIGE MUSTER
Keine CVE-spezifischen – Synology nennt keine Signaturen	DSM-Protokollcenter, Aufgabenplaner Benutzerkonten, Firewall-Logs	fremde Admin-Konten oder geplante Skripte Endung .L0CK3D, Notiz read-me3.txt

Zur Einordnung: Endung und Lösegeldnotiz stammen aus Berichten zur C3RB3R-Kampagne und zeigen eine bereits erfolgte Verschlüsselung, keinen Angriffsversuch. Die übrigen Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: NAS-Systeme stehen oft unbeachtet in Abteilungen und Filialen und tragen zugleich die Sicherungen. Wer sie verschlüsselt, trifft Daten und Wiederherstellung in einem Schritt.

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 neues Admin-Konto oder geplantes Skript auf dem NAS. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Synology-NAS mit offener DSM-Verwaltung 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 Synology DSM-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Prüfung auf Angriffsspuren, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Bestandsaufnahme aller Synology-NAS samt DSM-Build anordnen.
- Update auf den Fix-Build mit Termin einfordern.
- Prüfen lassen, ob Sicherungen getrennt vom NAS liegen.

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-2024-10441 und dem Synology DSM-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Synology-SA-24:20 (Fix-Builds, CVSS 9,8) · NVD · CISA KEV (18.11.2026) · Synology-Hinweis vom 29.10.2026 laut BleepingComputer. Stand 18.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.