AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-90436

Codeausführung ohne Anmeldung über Apache Axis 1.x.

Eine präparierte SOAP-Nachricht genügt, damit die veraltete Bibliothek Apache Axis 1.x fremden Code ausführt – ohne Anmeldung. Axis steckt in vielen Unternehmensanwendungen, unter anderem in Confluence Data Center. Apache liefert kein Update mehr; CISA führt die Lücke seit 18.11.2026 als aktiv ausgenutzt.

> **Geschäftsrisiko:** Übernahme des Anwendungsservers, Abfluss von Wiki-Inhalten, Datenbank- und Zugangsdaten sowie Ausbreitung ins Netz und in Cloud-Dienste – ein wahrscheinlich meldepflichtiger Vorfall nach DSGVO / NIS-2.

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. Basiswert von CISA (ADP) bei NVD; Atlassian bewertet für Confluence mit 9,3 (CVSS 4.0).

AKTIV AUSGENUTZT
CISA KEV seit 18.11.2026

BETROFFEN
Apache Axis 1.x bis 1.4 (EOL) – u. a. Confluence Data Center 1.x–9.x

HANDLUNGSBEDARF
Sofort – aktiv ausgenutzt

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Konto
SOAP-Anfrage genügt · CWE-470

Aktiv ausgenutzt
CISA KEV seit 18.11.2026

Kein Axis-Release
Fix je Produkt bzw. Migration

Die Ursache: Unsichere Reflexion (**CWE-470**): Enthält ein SOAP-Fehlerblock ein Element **exceptionName**, lädt Axis die dort genannte Java-Klasse und erzeugt sie mit Angreiferdaten, **bevor** geprüft wird, ob es überhaupt eine Fehlerklasse ist. Das geschieht schon bei der Zuordnung des Dienstes, also **vor jeder Anmeldeprüfung**. Mit einer passenden Klasse im Klassenpfad wird daraus Codeausführung.

ANGRIFFSKETTE

01	02	03	04
SOAP-Endpunkt – Angreifer erreicht einen Axis-Dienst im Netz	**Präparierter Fehlerblock** – exceptionName nennt eine fremde Klasse	**Klasse erzeugt** – Axis lädt sie vor jeder Anmeldeprüfung	**Codeausführung** – Befehle laufen als Dienstkonto der Anwendung

Betroffenheit & Fixversionen

Produkt	Verwundbar bis	Fixversion (Ziel)
Apache Axis 1.x	`bis 1.4 (EOL)`	kein Release – Migration
Confluence Data Center	1.x–9.x, Remote API an	`9.2.28 / 10.x`
N-able N-central	Legacy API aktiv	`2026.4.1.39 (HF3)`
Atlassian Cloud	nicht betroffen	–

Apache baut kein Axis-1.x-Release mehr; der Patch-Commit `41f3b4e` ist nur für Eigenbauten. Maßgeblich ist das Update **des Herstellers, der Axis mitliefert**. N-central laut Rapid7 eng korreliert.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf Systeme mit personenbezogenen Daten ist in der Regel meldepflichtig – 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

06.11.2026
Apache-Meldung + Patch-Commit

10.11.2026
Atlassian: Fix Confluence 9.2.28

13.11.2026
Angriffe auf Confluence (Rapid7)

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
SOAP-Zugang schließen	Produkte aktualisieren	Auf Einbruch prüfen

01 Betroffenheit feststellen

Anwendungen mit `axis-1.4.jar` bzw. Maven `axis:axis` erfassen, auch in Fremdsoftware. Bei Confluence Data Center prüfen, ob die Remote API (XML-RPC & SOAP) aktiv ist.

02 Aktualisieren oder ablösen

Confluence auf `9.2.28` oder 10.x, N-central auf `2026.4.1.39`. Eigene Axis-1-Dienste auf Axis2/Java oder eine andere SOAP-Lösung umstellen.

03 Zugang bis dahin schließen

In Confluence die Remote API abschalten und prüfen: `/plugins/servlet/soap-axis1/confluenceservice-v2` muss 403 liefern. In N-central die Legacy API deaktivieren.

04 Kompromittierung ausschließen

Logs auf unangemeldete POST-Aufrufe des SOAP-Endpunkts mit Status 500 prüfen, auf `bash/curl` unter dem Dienstkonto und auf Verbindungen zu Tunnel-Diensten.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Rapid7: IPs, trycloudflare-/pinggy-Tunnel, webhook.site – keine Datei-Hashes

AUSWERTUNGSQUELLEN

Zugriffslogs, Prozessliste, DNS/Proxy, Datenbank- und M365-Anmeldungen

AUFFÄLLIGE MUSTER

POST soap-axis1 mit HTTP 500
Java-Prozess startet bash/curl

Zur Einordnung: Die Indikatoren stammen aus einem von Rapid7 beobachteten Fall. IP-Adressen und Tunnel-Domains wechseln schnell; ihr Fehlen beweist nicht, dass ein System unberührt ist.

Wichtig: Axis 1.x ist seit Jahren abgekündigt und steckt oft unbemerkt in Fremdsoftware. Die Anmeldung eines Dienstes schützt nicht, weil der Fehler vorher greift.

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: Java-Prozess startet Shell nach SOAP-Aufruf. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Anwendungen mit Axis-1-SOAP-Endpunkt 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 Apache-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

- Klären lassen, wo Axis 1.x im Haus oder bei Dienstleistern läuft.
- Updates bzw. Abschaltung der SOAP-Schnittstelle mit Termin einfordern.
- Prüfung auf Kompromittierung anordnen, bevor entwarnt wird.

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-2026-90436 und dem Apache-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Apache-Advisory 06.11.2026 · CVE-Record · NVD (CVSS 9,8 CISA-ADP) · Atlassian-Advisory · Rapid7 · CISA KEV (18.11.2026). Stand 18.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.