AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2020-29574

Unauthentifizierte SQL-Injection in der Cyberoam-OS-WebAdmin.

Ein nicht authentifizierter Angreifer aus dem Netz kann über die WebAdmin-Oberfläche von Cyberoam OS beliebige SQL-Befehle einschleusen und ausführen. Damit lässt sich der Datenbestand der Firewall auslesen und manipulieren – in beobachteten Fällen wurden dabei unbekannte Administratorkonten angelegt. Die Schwachstelle steht seit Februar 2025 im CISA-Katalog aktiv ausgenutzter Lücken; Cyberoam OS ist ein abgekündigtes Produkt.

> **Geschäftsrisiko:** Vollständige Übernahme des Perimeter-Gateways: Anlegen versteckter Admin-Konten, Auslesen von Konfiguration und Zugangsdaten sowie Manipulation der Firewall-Regeln – mit Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO. Da das Produkt End-of-Life ist, besteht ohne Ablösung ein dauerhaftes Restrisiko.

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 Rechte, ohne Zutun – ein Angreifer kann beliebige SQL-Befehle gegen die Verwaltungsoberfläche der Firewall ausführen und so vollständige Kontrolle über Vertraulichkeit, Integrität und Verfügbarkeit erlangen. CVSS 2.0 bewertet die Lücke mit 7,5.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
6. Februar 2025	Cyberoam OS – alle Geräte ohne den Hotfix vom 04.12.2020	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Unauth SQLi
ohne Anmeldung ausführbar

Aktiv
ausgenutzt · CISA KEV (seit 06.02.2025)

End-of-Life
Cyberoam OS abgekündigt

Die Ursache: Die WebAdmin-Oberfläche von Cyberoam OS validiert in den betroffenen Ständen Eingaben nicht ausreichend, bevor sie in eine SQL-Abfrage einfließen. Ein **nicht authentifizierter** Angreifer aus dem Netz kann dadurch eigene SQL-Befehle in die Backend-Datenbank einschleusen, deren Inhalt auslesen und verändern – bis hin zum Anlegen eigener Administratorkonten.

ANGRIFFSKETTE

01	02	03	04
WebAdmin exponiert – die Cyberoam-Verwaltungsoberfläche ist über das Netz (WAN) erreichbar	**SQL einschleusen** – manipulierte, unauthentifizierte Anfrage an die anfällige WebAdmin	**Datenbank kompromittieren** – Auslesen und Verändern von Konfiguration und Zugangsdaten	**Persistenz** – Anlegen eines unbekannten Administratorkontos und dauerhafte Kontrolle über das Gateway

Betroffenheit & Fixversionen

Cyberoam-OS-Stand	Verwundbar bis	Fixversion (Ziel)
Cyberoam OS · alle Geräte	ohne Hotfix (bis 04.12.2020)	Hotfix ab 04.12.2020
Cyberoam OS · EOL-Versionen	10.6.2 und neuer, ohne Hotfix	Hotfix ab 04.12.2020
Empfohlene Ablösung	—	XG Firewall v17.5 / aktuelle Plattform

Betroffen sind Cyberoam-OS-Geräte, auf die der von Sophos automatisch ausgerollte Hotfix nicht aufgespielt wurde. Der Hotfix wurde ab dem `04.12.2020` an alle unterstützten Geräte sowie an die abgekündigten Versionen `10.6.2` und neuer verteilt. Cyberoam OS ist End-of-Life – Geräte, die vom Netz getrennt oder ohne automatische Update-Anbindung betrieben wurden, können den Hotfix nicht erhalten haben und bleiben verwundbar.

Regulatorischer Hinweis: Ein bestätigter Abfluss von Zugangsdaten oder personenbezogenen Daten oder ein kompromittiertes Perimeter-Gateway 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

04.12.2020
Sophos beginnt mit dem automatischen Ausrollen des Hotfix an Cyberoam-OS-Geräte

10.12.2020
Sophos veröffentlicht das Advisory (SOPHOS-SA-20201210) zur SQL-Injection

06.02.2025
CISA nimmt CVE-2020-29574 in den KEV-Katalog auf – aktive Ausnutzung

27.02.2025
KEV-Frist für US-Behörden zur Behebung bzw. Außerbetriebnahme

Ihr Maßnahmenplan.

In dieser Reihenfolge – Zugriff einschränken, Hotfix-Stand prüfen, auf Kompromittierung untersuchen, abgekündigte Geräte ablösen.

SOFORT	KURZFRISTIG	GEPLANT
WebAdmin/SSH aus dem WAN sperren	Hotfix-Stand prüfen, Admin-Konten auditieren	EOL-Gerät auf unterstützte Plattform ablösen

01 Betroffenheit feststellen

Prüfen, ob Cyberoam-OS-Geräte im Einsatz sind und ob deren WebAdmin- oder SSH-Zugang aus dem Internet (WAN) erreichbar ist. Da das Produkt End-of-Life ist, sind solche Geräte oft übersehene Altbestände.

02 Sofort mitigieren

Den Zugriff auf WebAdmin und SSH aus dem WAN unterbinden – unter `System > Administration > Appliance Access` die WAN-Zonen deaktivieren. Verwaltung nur noch aus vertrauenswürdigen internen Netzen zulassen.

03 Hotfix-Stand sicherstellen

Sicherstellen, dass der von Sophos ab dem `04.12.2020` ausgerollte Hotfix aufgespielt ist. Geräte, die zwischenzeitlich vom Netz getrennt waren oder ohne automatische Update-Anbindung liefen, gezielt auf den aktuellen Stand bringen.

04 Auf Kompromittierung prüfen

Alle Administrator- und Nutzerkonten auf der Firewall auf unbekannte oder unerwartete Einträge kontrollieren – das Anlegen eines unbekannten Admin-Kontos ist der von Sophos genannte Kompromittierungshinweis. Verdächtige Konten entfernen und Passwörter zurücksetzen.

05 Abgekündigtes Gerät ablösen

Cyberoam OS erhält keine reguläre Pflege mehr. Migration auf eine unterstützte Plattform (Sophos XG/XGS Firewall) einplanen, um das dauerhafte Restrisiko zu beseitigen.

Kompromittierungs-Indikatoren (IoCs)

KOMPROMITTIERUNGS-CHECK	AUFFÄLLIGE AKTIVITÄT	FOLGEINDIKATOREN
Unbekannte oder unerwartete Administratorkonten auf der Firewall	Unauthentifizierte Anfragen an die WebAdmin-Oberfläche aus fremden Quellen	Unerwartete Konfigurations- oder Regeländerungen am Gateway

Zur Einordnung: Das Anlegen eines unbekannten Administratorkontos ist der von Sophos konkret benannte Kompromittierungshinweis. Da die SQL-Injection über reguläre Web-Anfragen läuft, ist sie ohne detaillierte Zugriffs-Logs schwer zu erkennen – der zuverlässigste Indikator ist die Auswertung der WebAdmin-Zugriffs-Logs und ein vollständiges Audit der Firewall-Konten.

Wichtig: Der Hotfix wurde 2020 automatisch verteilt – das Risiko liegt heute vor allem bei Altgeräten, die zeitweise offline oder ohne Update-Anbindung waren und den Fix nie erhalten haben. Ein einmal angelegtes verstecktes Admin-Konto besteht auch nach dem Hotfix fort, solange es nicht gefunden und entfernt wird. Da Cyberoam OS End-of-Life ist, bleibt die Ablösung durch eine unterstützte Plattform die eigentliche Lösung.

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

24/7-SOC aus München: Anomale, unauthentifizierte Anfragen an die Cyberoam-WebAdmin und das Auftauchen unbekannter Administratorkonten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Netz erreichbare, nicht gepatchte Cyberoam-OS-Geräte 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 Cyberoam OS-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

- WebAdmin- und SSH-Zugriff auf Cyberoam-Geräte aus dem WAN heute sperren und den Hotfix-Stand verifizieren lassen.
- Alle Firewall-Konten auf unbekannte Administratoren auditieren und Zugangsdaten zurücksetzen lassen.
- Migration der End-of-Life-Cyberoam-Geräte auf eine unterstützte Plattform verbindlich einplanen.

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 vollständig 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-2020-29574 und dem Cyberoam OS-Perimeter.

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

Termin buchen

Quellen: Sophos Security Advisory SOPHOS-SA-20201210 (Cyberoam OS WebAdmin SQLi, veröffentlicht 10.12.2020, Hotfix ab 04.12.2020) · NVD (CVSS 3.1: 9,8 / CVSS 2.0: 7,5, CWE-89) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 06.02.2025, Frist 27.02.2025). Angaben nach bestem Wissen zum Stand 14.07.2026; Cyberoam OS ist End-of-Life – Ablösung durch eine unterstützte Plattform empfohlen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.