AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2022-1040

Authentifizierungs-Umgehung mit Codeausführung in Sophos Firewall.

Ein nicht authentifizierter Angreifer aus dem Netz kann die Anmeldung am User Portal und am Webadmin-Interface der Sophos Firewall vollständig umgehen und anschließend beliebigen Code auf der Appliance ausführen. Damit steht das zentrale Sicherheits-Gateway des Unternehmens unter fremder Kontrolle. Sophos hat die Schwachstelle bereits im März 2022 in gezielten Angriffen – vor allem auf Organisationen in Südasien – aktiv ausgenutzt beobachtet.

> **Geschäftsrisiko:** Vollständige Übernahme des Perimeter-Gateways: Der Angreifer kann Datenverkehr mitlesen und umleiten, VPN- und Verwaltungszugänge missbrauchen und tiefer ins Netz vordringen – mit Potenzial für Datenabfluss, Betriebsunterbrechung und einen 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 Rechte, ohne Zutun – die Anmeldung wird umgangen und beliebiger Code auf der Firewall ausgeführt, mit vollständigem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Eine CVSS-4.0-Bewertung liegt für diese Schwachstelle nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
März 2022	Sophos Firewall ≤ v18.5 MR3 (18.5.3)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Auth-Bypass + RCE
ohne Anmeldung ausführbar

Aktiv
ausgenutzt · CISA KEV (seit 31.03.2022)

User Portal / Webadmin
exponierte Web-Oberflächen

Die Ursache: In den betroffenen Versionen lässt sich die Authentifizierung am User Portal und am Webadmin-Interface der Sophos Firewall umgehen. Ein nicht authentifizierter Angreifer aus dem Netz kann dadurch geschützte Funktionen erreichen und über diese schließlich beliebigen Code auf der Appliance ausführen – ohne gültige Zugangsdaten und ohne Zutun eines Nutzers.

ANGRIFFSKETTE

01 **Oberfläche exponiert** – User Portal oder Webadmin ist über das WAN aus dem Netz erreichbar

02 **Anmeldung umgehen** – manipulierte, unauthentifizierte Anfrage überwindet die Authentifizierung

03 **Code ausführen** – über die freigeschaltete Funktion wird beliebiger Code auf der Firewall ausgeführt

04 **Ausweitung** – Verkehr abgreifen/umleiten, Zugangsdaten und VPN-Zugänge missbrauchen, weiter ins Netz vordringen

Betroffenheit & Fixversionen

Sophos-Firewall-Version (SFOS)	Verwundbar bis	Fixversion (Ziel)
SFOS 18.5	≤ 18.5 MR3 (18.5.3)	18.5 MR4 (18.5.4)
SFOS 19.0	EAP / Vorabversionen	19.0 GA
SFOS 17.0 · 17.5 · 18.0	unterstützte Zweige	Sophos-Hotfix

Betroffen sind alle Sophos-Firewall-Versionen bis einschließlich `v18.5 MR3 (18.5.3)`. Für alle unterstützten Zweige (17.0, 17.5, 18.0, 18.5, 19.0 EAP) hat Sophos ab dem 23. März 2022 Hotfixes ausgeliefert; den dauerhaften Fix enthalten `v18.5 MR4 (18.5.4)` und `v19.0 GA`. Bei aktivierter Option „Allow automatic installation of hotfixes" (Standard) wurde der Hotfix automatisch eingespielt – dies ist jedoch zu verifizieren.

Regulatorischer Hinweis: Die Übernahme eines Perimeter-Gateways ist regelmäßig als Sicherheitsvorfall zu bewerten. Ein bestätigter Abfluss personenbezogener 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

23.03.2022
Sophos liefert Hotfixes für die unterstützten Firewall-Zweige aus

25.03.2022
Sophos veröffentlicht Advisory SA-20220325 – aktive Ausnutzung in Südasien beobachtet

31.03.2022
CISA nimmt CVE-2022-1040 in den KEV-Katalog auf – aktive Ausnutzung

21.04.2022
KEV-Frist für US-Behörden zum Einspielen der Hersteller-Updates

Ihr Maßnahmenplan.

In dieser Reihenfolge – WAN-Zugriff abschalten, Hotfix/Update verifizieren, Kompromittierung ausschließen, Zugangsdaten rotieren.

SOFORT	KURZFRISTIG	PARALLEL
WAN-Zugriff auf User Portal / Webadmin sperren	Hotfix bzw. Update verifizieren	Threat Hunting / Kompromittierung prüfen

01 Betroffenheit feststellen

Prüfen, ob eine Sophos Firewall in einer Version bis einschließlich `v18.5 MR3 (18.5.3)` im Einsatz ist und ob User Portal oder Webadmin über das WAN erreichbar sind.

02 Sofort mitigieren

Den WAN-Zugriff auf User Portal und Webadmin nach den Device-Access-Best-Practices deaktivieren. Fernzugriff und Verwaltung stattdessen über VPN und/oder Sophos Central abwickeln. Von Sophos als Behelfsmaßnahme benannt.

03 Hotfix / Update verifizieren

Sicherstellen, dass der Hotfix eingespielt ist – bei aktivierter automatischer Hotfix-Installation geschieht dies standardmäßig. Anhand der Sophos-KB (KBA-000008204) verifizieren und auf eine dauerhaft gefixte Version aktualisieren: `v18.5 MR4 (18.5.4)` oder `v19.0 GA`.

04 Kompromittierung ausschließen

Da die Schwachstelle aktiv ausgenutzt wurde, die Firewall auf Anzeichen einer Übernahme prüfen: unbekannte Administrator-Konten, veränderte Konfiguration, ungewöhnliche VPN-Zugänge sowie anomale Zugriffe auf User Portal und Webadmin in den Logs.

05 Zugangsdaten rotieren

Bei Verdacht auf Kompromittierung alle Administrator- und Portal-Passwörter, VPN-Zugänge und API-/Verwaltungsgeheimnisse der betroffenen Firewall zurücksetzen – ein Patch macht bereits abgeflossene Geheimnisse nicht ungültig.

Kompromittierungs-Indikatoren (IoCs)

KONFIGURATIONS-CHECK

Unbekannte Administrator-Konten oder veränderte Firewall-/VPN-Konfiguration

AUFFÄLLIGE AKTIVITÄT

Unauthentifizierte Anfragen an User Portal / Webadmin aus fremden Quellen

FOLGEINDIKATOREN

Neu-/Fremdanmeldungen über VPN oder Verwaltungszugänge der Firewall

Zur Einordnung: Sophos nennt keinen einzelnen eindeutigen Datei-IoC. Da die Ausnutzung über reguläre Web-Anfragen an die exponierten Oberflächen läuft, ist der zuverlässigste Indikator die Auswertung Ihrer Zugriffs- und Firewall-Logs sowie ein Konfigurations-Review. Fehlende WAN-Logs erschweren die nachträgliche Erkennung.

Wichtig: Der Kern des Risikos liegt in der Exposition der Verwaltungs- und Portal-Oberflächen zum Internet: Ist die Firewall einmal übernommen, kann der Angreifer trotz späterem Patch über hinterlegte Konten und Zugänge zurückkehren. Deshalb ist – neben Hotfix und Update – die WAN-Sperre der Oberflächen und die Rotation der Zugangsdaten entscheidend.

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 Anfragen an User Portal / Webadmin sowie Konfigurations- und Kontenänderungen an der Firewall fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden über das WAN erreichbare, ungepatchte Sophos-Firewall-Oberflächen (User Portal / Webadmin) 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 Sophos Firewall-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

- WAN-Zugriff auf User Portal und Webadmin heute sperren; Verwaltung und Fernzugriff nur über VPN oder Sophos Central.
- Hotfix-Status verifizieren und auf eine dauerhaft gefixte Version (18.5.4 / 19.0 GA) aktualisieren lassen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist; bei Verdacht Zugangsdaten rotieren und den Vorgang dokumentieren.

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-2022-1040 und dem Sophos Firewall-Perimeter.

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

Termin buchen

Quellen: Sophos Security Advisory SA-20220325 (Resolved RCE in Sophos Firewall, CVE-2022-1040) · Sophos KB KBA-000008204 (Hotfix-Verifikation) · NVD (CVSS 3.1: 9,8 KRITISCH, Vektor AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H; keine CVSS-4.0-Bewertung) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 31.03.2022, Frist 21.04.2022).
Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.