AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2022-3236

Unauthentifizierte Code-Injection mit RCE in Sophos Firewall (User Portal / Webadmin).

Ein nicht authentifizierter Angreifer aus dem Netz kann über eine Code-Injection im User Portal und im Webadmin der Sophos Firewall beliebigen Code ausführen und damit das zentrale Perimeter-Gerät vollständig übernehmen. Betroffen sind SFOS-Versionen bis einschließlich v19.0 MR1. Sophos hat die aktive Ausnutzung gegen eine kleine Zahl gezielt angegriffener Organisationen – vorrangig in Südasien – beobachtet; die Schwachstelle steht im CISA-KEV-Katalog.

> **Geschäftsrisiko:** Vollständige Kompromittierung der Perimeter-Firewall: Angreifer können Datenverkehr mitlesen und umleiten, VPN- und Admin-Zugangsdaten abgreifen, Regeln manipulieren und sich tiefer ins Netz bewegen – 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 – vollständige Übernahme der Firewall durch Ausführung eigenen Codes mit voller Auswirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD bewertet die Lücke nach CVSS 3.1 mit 9,8.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
September 2022	Sophos Firewall (SFOS) v19.0 MR1 (19.0.1) und älter	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Unauth RCE
ohne Anmeldung ausführbar

Aktiv
ausgenutzt · CISA KEV (seit 23.09.2022)

CWE-94
Code-Injection

Die Ursache: Das User Portal und der Webadmin der Sophos Firewall validieren in den betroffenen Versionen Eingaben nicht ausreichend, bevor sie verarbeitet werden. Ein **nicht authentifizierter** Angreifer kann dadurch über die exponierten Web-Oberflächen eigenen Code einschleusen und auf dem Gerät zur Ausführung bringen – der Fehler ist als `CWE-94` (Improper Control of Generation of Code) eingestuft.

ANGRIFFSKETTE

01	02	03	04
Web-Oberfläche exponiert – User Portal oder Webadmin sind über das WAN/Internet erreichbar	**Code einschleusen** – manipulierte, unauthentifizierte Anfrage an den anfälligen Endpunkt	**Code ausführen** – der eingeschleuste Code wird auf der Firewall ausgeführt (RCE)	**Ausweitung** – Zugangsdaten und Konfiguration abgreifen, Regeln manipulieren, weiter ins Netz bewegen

Betroffenheit & Fixversionen

SFOS-Version	Verwundbar bis	Fixversion (Ziel)
SFOS v19.0	≤ `19.0 MR1 (19.0.1)`	`19.0 MR2 (19.0.2)`
SFOS v18.5	≤ `18.5 MR4`	`18.5 MR5 (18.5.5)`
SFOS v18.0 / v17.5 / v17.0 (ältere, teils EoL)	alle betroffen	Hotfix bzw. Upgrade auf unterstützte Version
SFOS v19.5 GA und neuer	nicht betroffen	—

Betroffen sind alle SFOS-Versionen bis einschließlich `v19.0 MR1 (19.0.1)`. Die permanenten Fixes sind `18.5 MR5`, `19.0 MR2` und `19.5 GA` und neuer; für ältere unterstützte Zweige (v17.0, v17.5, v18.0) hat Sophos Hotfixes bereitgestellt. Sophos verteilte den Hotfix automatisch an Geräte mit der Standardeinstellung „Allow automatic installation of hotfixes" – nicht mehr unterstützte oder von dieser Funktion abgekoppelte Geräte müssen manuell aktualisiert werden.

Regulatorischer Hinweis: Ein bestätigter Zugriff auf die Firewall oder ein Abfluss von Zugangsdaten bzw. 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

16.09.2022
Sophos entdeckt die Schwachstelle über das Bug-Bounty-Programm
CVE-2022-3236 · Überblick

23.09.2022
Sophos veröffentlicht Advisory (sophos-sa-20220923-sfos-rce); CISA nimmt CVE-2022-3236 in den KEV-Katalog auf

14.10.2022
KEV-Frist für US-Behörden zum Patchen/Absichern

Nov. 2023
Neue Ausnutzungsversuche gegen ältere, nicht mehr unterstützte Versionen; Advisory-Update

Seite 3: Ihr Maßnahmenplan →

Ihr Maßnahmenplan.

In dieser Reihenfolge – WAN-Zugriff abschalten, patchen, Zugangsdaten rotieren, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
WAN-Zugriff auf User Portal / Webadmin sperren	Patch/Hotfix einspielen, Zugangsdaten rotieren	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, ob eine Sophos Firewall in einer Version bis einschließlich `v19.0 MR1` im Einsatz ist und ob User Portal oder Webadmin vom WAN/Internet aus erreichbar sind. Genau diese Exposition macht die Lücke ausnutzbar.

02 Sofort mitigieren (vor dem Patch)

WAN-Zugriff auf User Portal und Webadmin deaktivieren und die Fernverwaltung stattdessen über VPN oder Sophos Central abwickeln – die von Sophos benannte Behelfsmaßnahme. Dies unterbindet die externe Ausnutzung sofort.

03 Patchen

Auf eine fehlerbereinigte Version aktualisieren – `18.5 MR5`, `19.0 MR2` oder `19.5 GA` und neuer. Bei aktivierter Standardfunktion „Allow automatic installation of hotfixes" auf unterstützten Versionen wurde der Hotfix bereits automatisch verteilt; dennoch aktiv verifizieren.

04 Zugangsdaten als kompromittiert behandeln

Bei möglicher Kompromittierung alle lokalen Admin- und Portal-Konten, VPN-Zugänge sowie API-/Dienst-Zugangsdaten der Firewall rotieren – ein Patch macht bereits abgeflossene Geheimnisse nicht ungültig.

05 Kompromittierung ausschließen

Konfiguration, Admin-Konten und Firewall-Regeln auf unbekannte Änderungen prüfen sowie Zugriffs- und Authentifizierungslogs auf anomale Anfragen an User Portal und Webadmin aus fremden Quellen durchsuchen.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE AKTIVITÄT

Unauthentifizierte Anfragen an `User Portal` / `Webadmin` aus fremden/WAN-Quellen

KONFIGURATIONS-CHECK

Unbekannte Admin-Konten, neue oder geänderte Firewall- und Zugriffsregeln

FOLGEINDIKATOREN

Neu-/Fremdanmeldungen über VPN oder Admin mit Firewall-Konten; abgehender C2-Verkehr

Zur Einordnung: Sophos hat keinen einzelnen eindeutigen technischen Indikator veröffentlicht. Da die Ausnutzung über reguläre Web-Anfragen an die exponierten Oberflächen läuft, ist sie ohne detaillierte Zugriffs-Logs schwer zu erkennen – der zuverlässigste Ansatz ist die Auswertung Ihrer Firewall-Zugriffs- und Authentifizierungslogs sowie ein Abgleich der Konfiguration gegen einen bekannten Soll-Stand.

Wichtig: Die Firewall ist das Perimeter-Kontrollgerät: Eine unauthentifizierte Code-Ausführung dort bedeutet die vollständige Übernahme des Netzübergangs. Selbst nach dem Patch bleiben zuvor abgeflossene Zugangsdaten – VPN, Admin, API – gültig. Deshalb ist die Rotation aller betroffenen Zugangsdaten ebenso wichtig wie das Update, und der WAN-Zugriff auf die Management-Oberflächen sollte grundsätzlich geschlossen bleiben.

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 und die Nutzung darüber abgeflossener Firewall-Zugangsdaten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte Sophos-Firewalls mit WAN-exponiertem 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 abschalten; Patch bzw. Hotfix-Status unverzüglich verifizieren.
- Alle Firewall-Zugangsdaten – Admin, Portal, VPN, API – rotieren lassen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.

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-2022-3236 und dem Sophos Firewall-Perimeter.

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

Termin buchen

Quellen: Sophos Security Advisory sophos-sa-20220923-sfos-rce (CVE-2022-3236) · NVD (CVSS 3.1: 9,8 KRITISCH, Vektor AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-94) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 23.09.2022, Frist 14.10.2022). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.