AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2020-12271

Pre-Auth-SQL-Injection in Sophos XG Firewall (Asnarök).

Eine nicht authentifizierte SQL-Injection in der Sophos XG Firewall erlaubt einem Angreifer aus dem Netz, lokal gespeicherte Zugangsdaten – Nutzernamen sowie gesalzene SHA256-Hashes der Admin- und Portal-Konten – auszulesen und Schadcode auszuführen. Die Lücke wurde bereits vor ihrer Veröffentlichung als Zero-Day für die Asnarök-Kampagne ausgenutzt: Die eingeschleuste Malware sammelte Zugangs- und VPN-Daten, verschlüsselte sie und versuchte, sie an einen externen Server zu übertragen. Verwundbar ist jedes Gerät, dessen Admin-Oberfläche (HTTPS) oder User-Portal auf der WAN-Zone erreichbar war.

> **Geschäftsrisiko:** Diebstahl von Firewall-Zugangsdaten und VPN-Konten, Fernausführung von Schadcode auf der Perimeter-Firewall und in der Folge unbefugter Zugriff auf das interne Netz – 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 – über eine SQL-Injection werden lokal gespeicherte Admin- und Nutzer-Zugangsdaten ausgelesen und Schadcode ausgeführt. CVSS 2.0 bewertet die Lücke mit 7,5.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
April 2020 (Zero-Day)	SFOS 17.0, 17.1, 17.5 und 18.0 vor dem Hotfix vom 25.04.2020 sowie ältere, nicht mehr unterstützte SFOS-Versionen	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Pre-Auth SQLi
ohne Anmeldung ausnutzbar

Aktiv
ausgenutzt · CISA KEV (seit 03.11.2021)

CWE-89
SQL-Injection

Die Ursache: SFOS neutralisiert in den betroffenen Versionen Eingaben an einem exponierten Web-Endpunkt nicht ausreichend, bevor sie in eine SQL-Abfrage einfließen. Ein nicht authentifizierter Angreifer kann dadurch eigene SQL-Befehle einschleusen, lokal gespeicherte Zugangsdaten auslesen und die Injection zur Fernausführung von Schadcode ausweiten. Voraussetzung ist, dass die Administrations-Oberfläche (HTTPS) oder das User-Portal auf der WAN-Zone erreichbar ist.

ANGRIFFSKETTE

01
Portal exponiert – Admin-Oberfläche (HTTPS) oder User-Portal ist über die WAN-Zone aus dem Netz erreichbar

02
SQL einschleusen – manipulierte, unauthentifizierte Anfrage schleust SQL-Befehle ein und weitet zur Codeausführung aus

03
Zugangsdaten auslesen – Nutzernamen, gesalzene SHA256-Hashes der Admin-/Portal-Konten und SSL-VPN-Nutzerlisten

04
Ausleiten (Asnarök) – Malware verpackt die Daten (tar), verschlüsselt sie (3DES) und versucht die Übertragung an einen externen Server

Betroffenheit & Fixversionen

SFOS-Version	Verwundbar bis	Fixversion (Ziel)
SFOS 18.0	vor Hotfix 25.04.2020	Hotfix (25.04.2020)
SFOS 17.5	vor Hotfix 25.04.2020	Hotfix (25.04.2020)
SFOS 17.1	vor Hotfix 25.04.2020	Hotfix (25.04.2020)
SFOS 17.0	vor Hotfix 25.04.2020	Hotfix (25.04.2020)
Ältere / nicht unterstützte SFOS	betroffen	auf unterstützte Version aktualisieren

Sophos hat den Fix am 25.04.2020 als Hotfix ausgeliefert, der auf allen unterstützten SFOS-Versionen mit aktivierter automatischer Hotfix-Installation selbsttätig eingespielt wurde. Geräte mit deaktivierter Automatik oder auf nicht mehr unterstützten Versionen sind nur nach manuellem Update bzw. Upgrade geschützt. Betroffen war ausschließlich, wessen Admin-Oberfläche (HTTPS) oder User-Portal auf der WAN-Zone exponiert war.

Regulatorischer Hinweis: Ein bestätigter Abfluss von Zugangsdaten oder 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

22.04.2020
Sophos erhält Meldung über einen auffälligen Wert im Management-

25.04.2020
Sophos liefert Hotfix aus (auf unterstützten SFOS-Versionen

26.04.2020
Sophos veröffentlicht die Asnarök-Analyse zur aktiven Ausnutzung

03.11.2021
CISA nimmt CVE-2020-12271 in den KEV-Katalog auf

03.05.2022
KEV-Frist für US-Behörden zum Patchen/Abschalten

Ihr Maßnahmenplan.

In dieser Reihenfolge – Exposition beenden, Hotfix/Update sicherstellen, Zugangsdaten rotieren, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
WAN-Exposition von Admin & User-	Hotfix/Update prüfen · Zugangsdaten	Threat Hunting / IoC-Abgleich ·

01 Exposition prüfen

Feststellen, ob die Administrations-Oberfläche (HTTPS) oder das User-Portal je auf der **WAN-Zone** erreichbar war. Nur so exponierte Geräte waren angreifbar. Admin-Dienste gehören generell nicht ins offene Netz.

02 Exposition sofort beenden

Zugriff auf Admin-Oberfläche und User-Portal aus dem WAN unterbinden bzw. auf autorisierte Hosts und Netze begrenzen. Fernadministration ausschließlich über VPN.

03 Hotfix / Update sicherstellen

Prüfen, dass der Sophos-Hotfix vom `25.04.2020` eingespielt ist; andernfalls manuell nachziehen. Nicht mehr unterstützte SFOS-Versionen auf eine aktuelle, unterstützte Version aktualisieren.

04 Zugangsdaten als kompromittiert behandeln

Da lokal gespeicherte Admin-, Portal- und Remote-Access-Konten (inkl. gesalzener SHA256-Hashes) ausgelesen werden konnten, alle betroffenen Passwörter und Konten rotieren – ein Patch macht bereits abgeflossene Geheimnisse nicht ungültig.

05 Kompromittierung ausschließen

Die von Sophos nach dem Hotfix ausgegebene Kompromittierungs-Anzeige des Geräts beachten, Verbindungen zur bekannten Exfiltrations-IP prüfen und das Gerät neu starten, um persistente Malware-Prozesse zu beenden.

```
grep 38.27.99.69 /log/*.log
```

Kompromittierungs-Indikatoren (IoCs)

EXFILTRATIONS-ZIEL

Ausgehende Verbindungen zu `38.27.99.69` (Asnarök-Datenabfluss)

KOMPROMITTIERUNGS-ANZEIGE

Sophos-Warnhinweis nach Hotfix, der das Gerät als potenziell kompromittiert markiert

FOLGEINDIKATOREN

Anomale Anfragen an Admin-/User-Portal und Neu-/Fremdanmeldungen mit lokalen SFOS-Konten

Zur Einordnung: Die von Sophos nach dem Hotfix eingeblendete Kompromittierungs-Anzeige ist der zuverlässigste Hinweis. Da die eigentliche SQL-Injection über reguläre Web-Anfragen läuft, ist sie ohne detaillierte Zugriffs-Logs schwer zu erkennen – werten Sie zusätzlich Firewall-, Web- und Authentifizierungs-Logs aus.

Wichtig: Der Kern des Risikos liegt nicht allein in der Codeausführung, sondern in den abgeflossenen Geheimnissen: Sind Admin-, Portal- und VPN-Zugangsdaten einmal exfiltriert, bleibt der Zugang auch nach dem Hotfix bestehen. Deshalb ist die Rotation aller betroffenen Zugangsdaten ebenso wichtig wie das Update – und die Admin-Oberfläche gehört dauerhaft aus dem offenen Netz.

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: Ausgehende Verbindungen zur Asnarök-Exfiltrations-IP sowie anomale Anfragen an Admin-Oberfläche und User-Portal fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden auf der WAN-Zone exponierte, ungepatchte SFOS-Instanzen 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 XG Firewall / SFOS-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

- Admin-Oberfläche und User-Portal heute aus dem WAN nehmen; Fernzugriff nur über VPN.
- Sicherstellen, dass der Sophos-Hotfix eingespielt bzw. auf eine unterstützte SFOS-Version aktualisiert ist.
- Alle lokal gespeicherten Firewall-, Portal- und VPN-Zugangsdaten rotieren und 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-2020-12271 und dem XG Firewall / SFOS-Perimeter.

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

Termin buchen

Quellen: Sophos Security Advisory / KB (Asnarök, KB-000039388) und Sophos-Blog „Asnarök“ (26.04.2020) · NVD (CVSS 3.1: 9,8 / CVSS 2.0: 7,5, CWE-89) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 03.11.2021, Frist 03.05.2022) · Rapid7 Analyse. Angaben nach bestem Wissen zum Stand 14.07.2026; Fix (Hotfix vom 25.04.2020 bzw. Upgrade auf eine unterstützte Version) gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.