AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2020-15069

Buffer Overflow mit Remote Code Execution im Sophos XG Firewall User Portal.

Ein nicht authentifizierter Angreifer aus dem Netz kann über die HTTP/S-Bookmark-Funktion des User Portals einen Pufferüberlauf auslösen und beliebigen Code auf der Firewall ausführen. Betroffen sind alle Sophos XG Firewalls unter SFOS v17.x, deren User Portal auf der WAN-Seite erreichbar ist. Sophos hat die Lücke bereits im Juni 2020 mit einem Hotfix geschlossen; die CISA hat sie im Februar 2025 als aktiv ausgenutzt in den KEV-Katalog aufgenommen.

> **Geschäftsrisiko:** Vollständige Kompromittierung des zentralen Perimeter-Schutzes: Wer die Firewall übernimmt, kontrolliert den Netzübergang, kann Datenverkehr mitlesen und umleiten und sich weiter ins interne 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 – ein Speicherüberlauf in der Bookmark-Funktion des User Portals erlaubt die Ausführung beliebigen Codes auf der Firewall, mit vollständigem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Die ältere CVSS-2.0-Bewertung liegt bei 7,5.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
6. Februar 2025 (CISA KEV)	SFOS 17.0 bis v17.5 MR12 (User Portal auf dem WAN erreichbar)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Unauth RCE
ohne Anmeldung ausführbar

Aktiv
ausgenutzt · CISA KEV (seit 06.02.2025)

CWE-120
Classic Buffer Overflow

Die Ursache: Die Firewall verarbeitet in den betroffenen SFOS-17.x-Versionen die Eingaben der HTTP/S-Bookmark-Funktion des **User Portals** (clientless access) nicht sicher: Es fehlt die Längenprüfung beim Kopieren in einen Speicherpuffer. Ein **nicht authentifizierter** Angreifer kann dadurch einen klassischen Pufferüberlauf (CWE-120) auslösen und beliebigen Code im Kontext der Firewall ausführen – vorausgesetzt, das User Portal ist über das WAN erreichbar.

ANGRIFFSKETTE

01	02	03	04
User Portal exponiert – das User Portal der XG Firewall ist auf der WAN-Seite erreichbar	**Bookmark missbrauchen** – manipulierte, unauthentifizierte Anfrage an die HTTP/S-Bookmark-Funktion	**Puffer überlaufen** – überlange Eingabe ohne Längenprüfung löst den Buffer Overflow aus	**Code ausführen** – beliebiger Code läuft auf der Firewall; von dort Ausweitung ins interne Netz

Betroffenheit & Fixversionen

SFOS-Version	Verwundbar bis	Fixversion (Ziel)
XG Firewall v17.x	`17.0 – v17.5 MR12`	`Hotfix HF062020.1`
XG Firewall v18	nicht betroffen	—

Betroffen sind ausschließlich Sophos XG Firewalls unter SFOS `v17.x` bis einschließlich `v17.5 MR12`, deren User Portal auf dem WAN erreichbar ist. XG Firewall `v18` ist von dieser Schwachstelle nicht betroffen. Sophos hat den Hotfix `HF062020.1` automatisch an alle v17.x-Geräte verteilt, sofern die automatische Hotfix-Installation aktiviert war.

Regulatorischer Hinweis: Die vollständige Übernahme einer Perimeter-Firewall kann einen meldepflichtigen Sicherheitsvorfall auslösen; bei bestätigtem Abfluss personenbezogener Daten greift die DSGVO-Meldepflicht 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

25.06.2020
Sophos veröffentlicht Advisory und Hotfix HF062020.1 für alle v17.x-Geräte

29.06.2020
NVD veröffentlicht CVE-2020-15069 (CVSS 3.1: 9,8, CWE-120)

06.02.2025
CISA nimmt CVE-2020-15069 in den KEV-Katalog auf – aktive Ausnutzung

27.02.2025
KEV-Frist für US-Behörden zum Patchen/Abschalten

Ihr Maßnahmenplan.

In dieser Reihenfolge – User Portal vom WAN nehmen, Hotfix/Upgrade sicherstellen, Zugangsdaten rotieren, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
User Portal vom WAN trennen	Hotfix prüfen / auf v18 upgraden	Konten zurücksetzen · Threat Hunting

01 Betroffenheit feststellen

Prüfen, ob eine XG Firewall unter SFOS `v17.x` (bis `v17.5 MR12`) im Einsatz ist und ob das User Portal auf der WAN-Seite erreichbar ist. Nur diese Konstellation ist aus dem Internet angreifbar.

02 Sofort mitigieren (vor dem Patch)

Den Zugriff auf das **User Portal** von der WAN-Seite deaktivieren, sofern er nicht zwingend benötigt wird. Von Sophos als zentrale Behelfsmaßnahme benannt – sie entzieht dem Angriff die Angriffsfläche.

03 Patchen / upgraden

Sicherstellen, dass der Hotfix `HF062020.1` installiert ist (automatische Hotfix-Installation aktivieren). Empfohlen wird zusätzlich das Upgrade auf `SFOS v18`, das von dieser Schwachstelle nicht betroffen ist.

04 Zugangsdaten als kompromittiert behandeln

Sophos empfiehlt, die Passwörter aller Geräte-Administrator-Konten und lokalen Benutzerkonten zurückzusetzen – ein Patch macht bereits abgeflossene oder gesetzte Zugangsdaten nicht ungültig.

05 Kompromittierung ausschließen

Firewall-Logs und Konfiguration auf unbekannte Administratoren, geänderte Regeln und anomale Anfragen an das User Portal prüfen. Bei Verdacht das Argos-CDC / Incident-Response hinzuziehen.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE AKTIVITÄT

Unerwartete oder überlange Anfragen an die HTTP/S-Bookmark-Funktion des User Portals

KOMPROMITTIERUNGS-CHECK

Neue oder unbekannte Administrator-Konten, unerklärte Änderungen an Firewall-Regeln

FOLGEINDIKATOREN

Ungewöhnliche ausgehende Verbindungen der Firewall oder Bewegungen ins interne Netz

Zur Einordnung: Ein spezifischer, öffentlich dokumentierter Netzwerk-IoC für diese Lücke liegt nicht belastbar vor. Der zuverlässigste Nachweis ist die Auswertung Ihrer Firewall- und User-Portal-Zugriffslogs sowie der Abgleich der Administrator- und Benutzerkonten mit dem Soll-Zustand.

Wichtig: Der Kern des Risikos ist die Erreichbarkeit des User Portals aus dem Internet: Ist es auf dem WAN exponiert und läuft SFOS v17.x ohne Hotfix, ist die Firewall unauthentifiziert übernehmbar. Deshalb sind das Abschalten des WAN-Zugriffs und das Zurücksetzen der Konten ebenso wichtig wie der Hotfix bzw. das Upgrade auf v18.

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 das User Portal der XG Firewall und ungewöhnliche Aktivität der Firewall im internen Netz fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare, ungepatchte XG Firewalls unter SFOS v17.x mit WAN-seitigem User Portal 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-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

- User-Portal-Zugriff vom WAN heute deaktivieren, wo nicht zwingend nötig.
- Hotfix HF062020.1 verifizieren oder auf SFOS v18 upgraden; automatische Hotfix-Installation aktivieren.
- Administrator- und lokale Benutzerkonten zurücksetzen 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-2020-15069 und dem XG Firewall-Perimeter.

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

Termin buchen

Quellen: Sophos Security Advisory sophos-sa-20200625-xg-user-portal-rce (Hotfix HF062020.1, Upgrade auf v18) · NVD CVE-2020-15069 (CVSS 3.1: 9,8 KRITISCH, Vektor AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H; CVSS 2.0: 7,5; CWE-120) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 06.02.2025, Frist 27.02.2025). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.