AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2023-1671

Unauthentifizierte Befehlseinschleusung in Sophos Web Appliance.

Ein nicht authentifizierter Angreifer aus dem Netz kann über den „Warn-Proceed"-Handler der Sophos Web Appliance eigene Betriebssystembefehle einschleusen und beliebigen Code ausführen – ganz ohne Anmeldung. Damit steht die Appliance und der über sie laufende Web-Verkehr offen. Die Schwachstelle wird seit November 2023 aktiv ausgenutzt und steht im CISA-KEV-Katalog. Erschwerend kommt hinzu, dass die Sophos Web Appliance bereits am 20. Juli 2023 das Ende ihrer Lebensdauer erreicht hat.

> **Geschäftsrisiko:** Vollständige Übernahme eines exponierten Sicherheits-Gateways, in der Folge Manipulation des Web-Verkehrs, Ausspähen von Zugangsdaten und ein Brückenkopf ins 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 – vollständige Ausführung beliebiger Befehle auf der Appliance mit Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Eine CVSS-4.0-Bewertung liegt beim NVD nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
16. November 2023	Sophos Web Appliance < 4.3.10.4	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Pre-Auth RCE
ohne Anmeldung, Codeausführung

Aktiv
ausgenutzt · CISA KEV (seit 16.11.2023)

CWE-77
Command Injection

Die Ursache: Der „Warn-Proceed"-Handler der Sophos Web Appliance verarbeitet Anfragen an den Endpunkt `/index.php?c=blocked&action=continue`. Der dabei übergebene, Base64-kodierte Parameter `user_encoded` wird dekodiert und an ein Shell-Kommando weitergereicht, ohne ausreichend neutralisiert zu werden. Ein **nicht authentifizierter** Angreifer kann so aus den Argumenten ausbrechen und eigene Betriebssystembefehle einschleusen, die mit den Rechten des Dienst-Nutzers `spiderman` ausgeführt werden.

ANGRIFFSKETTE

01
SWA exponiert – das Web-Interface der Appliance ist über das Netz erreichbar

02
Warn-Proceed ansprechen – unauthentifizierte POST-Anfrage an `/index.php?c=blocked&action=continue`

03
Befehl einschleusen – der Base64-kodierte `user_encoded`-Parameter bricht aus dem Shell-Argument aus

04
Codeausführung – beliebige Befehle als Nutzer `spiderman`, z. B. Reverse Shell und Übernahme der Appliance

Betroffenheit & Fixversionen

SWA-Version	Verwundbar bis	Fixversion (Ziel)
Sophos Web Appliance	< 4.3.10.4	4.3.10.4
SWA (nach 20.07.2023)	End-of-Life – keine Updates	Migration

Betroffen sind alle Versionen der Sophos Web Appliance unterhalb `4.3.10.4`. Der Fix wird laut Sophos automatisch verteilt – vorausgesetzt, die Appliance ist online und der Auto-Update-Mechanismus aktiv. Entscheidend: Die Sophos Web Appliance hat am **20. Juli 2023** ihr Lebensende erreicht und erhält seither keine Sicherheits- oder Software-Updates mehr. Eine dauerhafte Absicherung ist nur durch Migration auf ein unterstütztes Produkt möglich.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder 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

04.04.2023
Sophos veröffentlicht Advisory (sophos-sa-20230404-swa-rce), Fix 4.3.10.4 automatisch verteilt

20.07.2023
Sophos Web Appliance erreicht das Ende der Lebensdauer (End-of-Life)

16.11.2023
CISA nimmt CVE-2023-1671 in den KEV-Katalog auf – aktive Ausnutzung

Nov. 2023
VulnCheck veröffentlicht technische Analyse und PoC-Details, öffentlicher Exploit verfügbar

07.12.2023
KEV-Frist für US-Behörden zum Patchen/Abschalten

Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit prüfen, Netzzugriff abriegeln, Fixstand verifizieren, Kompromittierung ausschließen, Migration einleiten.

01 Betroffenheit feststellen

Prüfen, ob eine Sophos Web Appliance im Einsatz ist und ob ihr Web-Interface über das Netz – insbesondere aus dem Internet – erreichbar ist. Als reines Web-Gateway ist die Appliance häufig genau dort exponiert, wo sie am verwundbarsten ist.

02 Sofort mitigieren (Erreichbarkeit)

Die Appliance hinter eine Firewall stellen und den Zugriff auf das Verwaltungs-/Web-Interface strikt auf autorisierte Hosts und Netze begrenzen – keinesfalls aus dem öffentlichen Internet erreichbar. Von Sophos ausdrücklich empfohlen.

03 Fixstand verifizieren

Sicherstellen, dass die Appliance auf `4.3.10.4` oder neuer läuft. Der Fix wird per Auto-Update verteilt – das gilt aber nur für Instanzen, die online und mit aktivem Update-Mechanismus betrieben werden. Offline- oder stillgelegte Geräte manuell abgleichen.

04 Kompromittierung ausschließen

Die Zugriffslogs auf verdächtige Anfragen an den anfälligen Endpunkt durchsuchen und nach ungewöhnlichen Prozessen der Appliance Ausschau halten. Bei Treffern von einer Kompromittierung ausgehen und den Vorfallsprozess starten.

```
grep 'c=blocked&action=continue'
/log/ui_access_log
```

05 Migration einleiten

Da die Sophos Web Appliance seit dem 20.07.2023 End-of-Life ist und keine weiteren Sicherheitsupdates erhält, den Umstieg auf ein unterstütztes Web-Protection-Produkt planen. Ein einzelner Patch schützt nicht vor künftigen, dann ungefixten Lücken.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE ANFRAGE

POST auf `/index.php?c=blocked&action=continue` mit Base64-Wert im `user_encoded`-Parameter

LOG-SPUR

Passende Einträge in `/log/ui_access_log` aus fremden oder unerwarteten Quellen

PROZESS-SPUR

Shell-/Reverse-Shell-Aktivität als Nutzer `spiderman` im Umfeld von `ftsblistpack` / `sblistpack`

Zur Einordnung: Die Log-Auswertung ist der zuverlässigste Nachweis: Die Ausnutzung läuft über eine regulär aussehende Web-Anfrage und ist ohne Zugriffs-Logs schwer zu erkennen. Prüfen Sie /log/ui_access_log auf Anfragen an den Warn-Proceed-Endpunkt und korrelieren Sie mit ungewöhnlicher Prozess- und Netzaktivität der Appliance.

Wichtig: Der Kern des Risikos liegt in der Kombination aus aktiver Ausnutzung und End-of-Life: Ein einzelner automatischer Fix schließt zwar diese Lücke, doch die Sophos Web Appliance erhält seit dem 20.07.2023 grundsätzlich keine Sicherheitsupdates mehr. Wer sie weiterbetreibt, bleibt gegenüber künftigen Schwachstellen dauerhaft ungeschützt – die einzige nachhaltige Maßnahme ist die Migration auf ein unterstütztes Produkt.

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 den Warn-Proceed-Endpunkt der Appliance und darauf folgende Shell-/Reverse-Shell-Aktivität als Nutzer spiderman fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte oder End-of-Life-Sophos-Web-Appliances 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 Web Appliance-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

- Sophos Web Appliance heute vom Internet trennen und hinter eine Firewall stellen; Fixstand 4.3.10.4 verifizieren lassen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung nach NIS-2 / DSGVO.
- Migration auf ein unterstütztes Web-Protection-Produkt einplanen; die Appliance ist seit Juli 2023 End-of-Life.

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-2023-1671 und dem Web Appliance-Perimeter.

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

Termin buchen

Quellen: Sophos Security Advisory sophos-sa-20230404-swa-rce (CVE-2023-1671) · 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-77; CVSS 4.0 nicht bewertet) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 16.11.2023, Frist 07.12.2023) · VulnCheck Attack Research (technische Analyse, PoC). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.