Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Gefahr durch Remote Code Execution - Kritische Schwachstelle in Sophos Firewalls wird aktiv ausgenutzt

Nr. 2022-258025-1022, Version 1.0, 26.09.2022

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 23. September 2022 veröffentlichte das IT-Sicherheitsunternehmen Sophos ein Advisory auf seiner Webseite [SOPH2022a], in dem Kunden über eine neu entdeckte Schwachstelle in Firewalls des Unternehmens informiert werden.

Auf Basis der nach Common Vulnerability Scoring System (CVSS) v3.1 mit 9.8 als „kritisch“ bewerteten Sicherheitslücke ist ein entfernter, nicht authentisierter Angreifer in der Lage, aus der Ferne Code auszuführen und somit ggf. Informationen abzugreifen oder das Gerät zu übernehmen. Voraussetzung ist jedoch ein Zugriff auf das Sophos User Portal bzw. Webadmin. In den Common Vulnerabilities and Exposures (CVE) wird die Schwachstelle unter der Nummer CVE-2022-3236 geführt.

Betroffen sind Geräte, auf denen das Sophos Firewall Operating System (SFOS) in der Version v19.0 MR1 (19.0.1) oder älter zum Einsatz kommt.

Dem Hersteller zufolge wurden bereits Attacken beobachtet, die sich derzeit jedoch auf den asiatischen Raum beschränken.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bewertung

Firewalls stellen aufgrund ihrer zentralen Bedeutung für die IT-Infrastruktur attraktive Ziele für Cyber-Angriffe dar.

Gleichzeitig belegt die bereits stattfindende Ausnutzung der Schwachstellen die erhöhte Notwendigkeit für IT-Sicherheitsverantwortliche, Schutzmaßnahmen zu ergreifen bzw. zu prüfen. Zwar wird bislang nur von einer Ausnutzung in Asien berichtet, die kurzfristige Durchführung von Angriffen in Deutschland kann jedoch nicht ausgeschlossen werden.

Maßnahmen

Sophos stellt für die Software-Versionen 17.0 bis 19.0 Hotfixes zur Verfügung. Sofern die automatische Installation von Hotfixes aktiviert ist, sind keine weiteren Schritte notwendig. Falls dieses Feature nicht genutzt wird, sollten IT-Sicherheitsverantwortliche eine Installation kurzfristig prüfen.

Institutionen, die ältere, nicht mehr unterstützte Software-Versionen nutzen, empfiehlt der Hersteller ein Upgrade auf eine aktuelle SFOS-Version.

Darüber hinaus sollte grundsätzlich verhindert werden, dass ein unautorisierter Zugriff auf User Portal und Webadmin möglich ist – z.B. durch die Anbindung per VPN. Empfehlungen für die sichere Konfiguration aus der Ferne können den Herstellerempfehlungen [SOPH2022b] oder dem BSI IT-Grundschutz [BSI2022] entnommen werden.

Links

[SOPH2022a] Resolved RCE in Sophos Firewall (CVE-2022-3236): https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce

[SOPH2022b] Sophos Firewall Device access: https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.html

[BSI2022] BSI IT-Grundschutz NET.3.2 – Firewall: https://bsi.bund.de/dok/989066

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.