TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
NUEVA EXPLOTACIÓN ACTIVA DE VULNERABILIDAD EN FIREWALL SOPHOS

1. Antecedentes generales.

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, advierte de una nueva campaña de explotación activa de una vulnerabilidad en Sophos Firewall.

El CSIRT de Gobierno considera que existe evidencia suficiente para alertar a la comunidad del Estado sobre la explotación activa de la vulnerabilidad identificada como CVE-2022-3236, la que fue recientemente advertida por el fabricante y ha sido catalogada como crítica.

Esta campaña se suma a la nueva advertencia realizada este viernes 23 de septiembre sobre una vulnerabilidad publicada en marzo pasado e informada oportunamente por el CSIRT sobre este mismo firewall (CVE-2022-1040), de la cual se tienen antecedentes de intentos de explotación en Chile.

Dado que ambas vulnerabilidades apuntan al Sophos Firewall y por la actividad maliciosa detectada, es que CSIRT solicita aplicar con urgencia los parches de seguridad liberados por el fabricante y cuyos enlaces se encuentran al final de este documento.

2. Vulnerabilidad.

La nueva vulnerabilidad crítica (CVE-2022-3236), afecta al Firewall Sophos v19.0 MR1 (19.0.1) y las versiones anteriores.

La vulnerabilidad de inyección de códigos permite a los atacantes la inyección de código remoto en los componentes “User Portal” y “Webadmin”.

La descripción de la explotación de esta vulnerabilidad es similar al comportamiento de los atacantes advertidos en los incidentes recientemente reportados en Chile.

3. Recomendaciones

El CSIRT de Gobierno recomienda a las organizaciones implementar las siguientes medidas:

- Actualizar la vulnerabilidad del Firewall Sophos informada por el fabricante
- Verificar el historial de los logs de acceso para identificar si existe algún sistema comprometido
- Verificar todas las reglas en el Firewall que sean sospechosas
- Verificar la creación de túneles VPN
- Verificar los entornos lógicos que se encuentren al alcance de la red (servidores, sitios web, servidores de correo, servidores de datos etc.) donde se encuentra el Firewall

- Crear sistemas de correlación de eventos para detectar anomalías en la configuración de seguridad de los equipos perimetrales
- Asegurarse de contar con respaldos de las configuraciones de los dispositivos de internet crítico (DNS, Switch, Firewall, etc.)

4. Enlaces.

El CSIRT de Gobierno comparte los enlaces con la información de las vulnerabilidades y los parches respectivos:

- Parche para nueva vulnerabilidad crítica **CVE-2022-3236**
  Enlace de CSIRT: https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00706-01/
  Enlace del fabricante: https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce
  Enlace NIST: https://nvd.nist.gov/vuln/detail/CVE-2022-3236

- Para vulnerabilidad CVE-2022-1040
  Enlace de CSIRT: https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00601-01/
  Alerta liberada por CSIRT 23 de septiembre, 10CND22-00078-01 con **Indicadores de compromiso**: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-sophos/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.24 14:56:20 -03'00'