TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
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, recibió antecedentes sobre un incidente en una entidad de la economía nacional que fue contenida oportunamente.

El incidente fue reportado en tiempo y oportunidad al regulador respectivo, siguiendo las normas técnicas acordadas y suscritas con ese sector de la economía en años recientes.

La exitosa respuesta del incidente no solo evitó que los atacantes pudieran explotar la vulnerabilidad, sino que ha permitido reunir algunos Indicadores de Compromiso (IoC) que compartimos con la comunidad en este informe.

2. Incidente.

El incidente se manifestó a mediados de este mes, pero de acuerdo con lo informado por la entidad afectada, el actor de amenaza habría explorado los sistemas vulnerables de la entidad desde el pasado mes de agosto.

El atacante pudo acceder al Firewall del sistema aprovechando una vulnerabilidad sin parchar advertida por el fabricante y el CSIRT de gobierno desde marzo de 2021.

El ataque fue contenido y el atacante expulsado de los sistemas que se vieron afectados. Los servicios de la entidad afectada no fueron suspendidos y no hubo datos afectados.

La entidad afectada actuó adecuadamente durante el incidente y con posterioridad, informando a las entidades que regulan el sector específico en el que se desarrolla su actividad.

La entidad adoptó una serie de medidas de mitigación y de mejora de sus sistemas y manifestó a través de sus representantes, la posibilidad de implementar nuevas mejoras para proteger sus sistemas, compartimentar su información y mantener respaldos.

3. Vulnerabilidad.

La vulnerabilidad vinculada al incidente fue identificada como CVE-2022-1040 para Sophos Firewall, y fue informada por el fabricante y advertida por CSIRT el pasado mes de marzo de 2022 en el documento https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00601-01/.

Esta vulnerabilidad existe debido a una validación insuficiente del input del usuario en el User Portal y en Webadmin. Un atacante remoto puede enviar solicitudes especialmente diseñadas a la interfaz web y ejecutar código arbitrario en el sistema. La explotación exitosa de la vulnerabilidad podría permitir a un atacante comprometer el equipo afectado, como se intentó en el caso que se describe en este documento.

El CSIRT de Gobierno considera que existe evidencia de explotación activa de esta vulnerabilidad y advierte a las organizaciones para que apliquen los parches de seguridad lo antes posible.

4. Indicadores de Compromiso

La acción de la entidad durante el ataque permitió identificar los siguientes IoC:

- 66.187.6.55 (USA)
- 66.187.6.56 (USA)
- 85.106.108.76 (Turquía)
- 85.106.108.77 (Turquía)
- 45.134.144.213 (Alemania)
- 185.159.80.80 (Países Bajos)
- 65.21.187.40 (Finlandia)
- 85.114.102.98 (Israel)
- 45.143.223.162 (Belice)

5. Recomendaciones

El CSIRT de Gobierno recomienda a las organizaciones implementar lo siguiente:

- 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.)