Alerta de seguridad cibernética	9VSA20-00189-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2020
Última revisión	27 de abril de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Sophos referente a vulnerabilidad que afecta a Sophos XG Firewall/SFOS. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDAD

CWE-89

CWE-89

Debido a la insuficiente sanitización de datos ingresados por el usuario entregados en el portal de usuario o en las interfaces de administrador, un atacante remoto no autenticado podría enviar a la aplicación, peticiones especialmente diseñadas y ejecutar comandos SQL en la base de datos.
Una explotación exitosa permitiría leer, modificar y hasta eliminar datos en la base de datos, comprometiendo completamente al sistema afectado.

Productos Afectados

XG Firewall virtual y físico versiones: 15.0, 15.01, 16.01, 16.01.2, 16.01.3, 16.05.0, 16.05.1, 16.05.2, 16.05.3, 16.05.4, 16.05.5, 16.05.6, 16.05.7, 16.05.8, 17.0.0, 17.0.1, 17.0.2, 17.0.3, 17.1, 17.5 y 18.0

Mitigación

Aplicar los parches publicados por los desarrolladores.

Enlaces

https://community.sophos.com/kb/en-us/135412