

Alerta de seguridad cibernética	9VSA22-00706-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	24 de septiembre de 2022
Última revisión	24 de septiembre de 2022

## 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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afectada a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre una nueva vulnerabilidad crítica comunicada por Sophos.

## Vulnerabilidad

CVE-2022-3236

## Impacto

### Vulnerabilidades de riesgo alto

CVE-2022-3236: Vulnerabilidad de inyección de código que permite la ejecución remota de código. Sophos indica que ya ha sido explotada en el Sudeste Asiático.

### Productos afectados

Sophos Firewall v19.0 MR1 (19.0.1) y anteriores.

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Enlaces

<https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3236>