

Alerta de seguridad cibernética	9VSA21-00358-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	09 de enero de 2021
Última revisión	09 de enero de 2021

## 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 PHP sobre vulnerabilidades que afectan a su lenguaje de scripts.

Este informe incluye las medidas de mitigación, consistentes en instalar las últimas actualizaciones de los productos afectados.

## Vulnerabilidad

CVE-2020-7071

## Impacto

Esta vulnerabilidad permite a un atacante remoto el evadir las restricciones de seguridad implementadas. La vulnerabilidad existe debido a una validación insuficiente de las URL efectuadas a través de la configuración "FILTER\_VALIDATE\_URL".

### Productos Afectados

PHP: Versiones de la 7.3 a la 7.4.13.

### Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

### Enlaces

<https://bugs.php.net/bug.php?id=77423>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7071>