Alerta de seguridad informática	9VSA20-00138-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de febrero de 2020
Última revisión	10 de febrero 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 información obtenida de PHP, referente a múltiples vulnerabilidades la cuales de ser explotadas, permitirían a un atacante realizar ataques de denegación de servicios y acceder a información potencialmente sensible. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-7059

CVE-2020-7060

Impactos

Un atacante remoto podría realizar ataques de denegación de servicios y obtener información potencialmente sensible debido a una condición de lectura fuera de la memoria al utilizar la función "fgetss()" para leer datos o "mbstring" para convertir ciertos datos.
Al explotar estas funciones un atacante podría leer datos en memoria y botar la aplicación.

Productos Afectados

PHP desde la versión 7.2.0 hasta la 7.4.1.

Mitigación

Actualizar a la versión publicada por el fabricante.

Enlaces

https://bugs.php.net/bug.php?id=79099
https://bugs.php.net/bug.php?id=79037
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7059
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7060