Alerta de seguridad informática	9VSA-00070-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de octubre de 2019
Última revisión	28 de octubre de 2019

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 obtenida de diferentes fuentes, referente a una vulnerabilidad en PHP7 al ser utilizado en NGINX o PHP-FPM, junto a su respectiva forma de mitigarla.

Vulnerabilidad

CVE-2019-11043

Impacto

Esta vulnerabilidad es de tipo ejecución de código remoto, se aprovecha de un error en *underflow memory corruption* en <<*env_path_info*>> en el módulo PHP-FMP, el cual permite al atacante tomar control del servidor vulnerable.

Productos Afectados

Las versiones anteriores a las mencionadas en Mitigación son vulnerables en su configuración si:

- Utiliza NGINX y reenvía peticiones al procesador PHP-FPM.
- Configura 'fast_split_path_info' con una expresión regular que comience con '^' y termine con '$'.
- La variable PATH_INFO está definida con fastcgi_param.
- No hay comprobaciones como try_files $ uri = 404 o if (-f $ uri) que determinen si un archivo existe o no.

Mitigación

Actualizar a la versión PHP 7.3.11 ó PHP 7.2.24.

Enlace

- https://bugs.php.net/bug.php?id=78599
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11043