Alerta de seguridad informática	9VSA20-00161-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de marzo de 2020
Última revisión	21 de marzo 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 que afectan a sus componentes, las cuales de ser explotadas permitirían a un atacante remoto obtener acceso a información potencialmente sensible, evadir ciertas medidas de seguridad y hasta comprometer completamente al sistema afectado. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-7064

CVE-2020-7066

CVE-2020-7065

Impactos

CVE-2020-7064

Debido a un error en memoria (out-of-bounds read) con la función PHP “exif_read_data()”, un atacante podría enviarle datos maliciosos a la aplicación, causar el error en memoria y lograr acceder a datos en esta.

CVE-2020-7066

Debido a que la función PHP “get_headers()” trunca silenciosamente los encabezados después de recibir un carácter “NULL byte”, un atacante podría abusar de este comportamiento para evadir restricciones de seguridad implementadas en el sistema.

CVE-2020-7065

Debido a un error en memoria (stack-based buffer overflow) con la función PHP “php_unicode_tolower_full()”, demostrado por la llamada “mb_strtolower()”, un atacante podría enviar datos maliciosos a la aplicación que utiliza la función afectada, gatillar el error en memoria y lograr la ejecución de código arbitrario en el sistema, permitiéndole comprometerlo completamente.

Producto Afectado

Para la versión 7.2, actualizar a la 7.2.29.
Para la versión 7.3, actualizar a la 7.3.16.
Para la versión 7.4, actualizar a la 7.4.4.

Mitigación

PHP 7.2 desde la versión 7.2.0 hasta la 7.2.28.
PHP 7.3 desde la versión 7.3.0 hasta la 7.3.15.
PHP 7.4 desde la versión 7.4.0 hasta la 7.4.3.

Enlaces

https://bugs.php.net/bug.php?id=79282
https://www.php.net/ChangeLog-7.php#7.2.29
https://www.php.net/ChangeLog-7.php#7.3.16
https://www.php.net/ChangeLog-7.php#7.4.4
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7064
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7066
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7065