Alerta de seguridad cibernética	9VSA20-00266-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de julio de 2020
Última revisión	09 de julio 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 la información obtenida de PHPMailer respecto a vulnerabilidad que afecta a su servidor de correo. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-13625

CVE-2020-13625

Es posible engañar a filtros de correo modificando el nombre del archivo adjunto, en donde la utilizar el nombre ’filename.html";.jpg', el formato del archivo sería HTML en vez de JPG (la última parte sería ignorada), por lo que si ciertos filtros no permitían un tipo de archivo, se podía utilizar este método para enviar un tipo válido y evadir las medidas de seguridad.

Productos Afectados

PHPMailer versión 6.1.5 y anteriores.

Mitigaciones

Actualizar a la versión 6.1.6 de PHPMailer.

Enlaces

https://github.com/PHPMailer/PHPMailer/security/advisories/GHSA-f7hx-fqxw-rvvj
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13625