

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad informática | 9VSA20-00117-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de enero de 2020 |
| Última revisión | 11 de enero 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 phpMyAdmin, referente a una vulnerabilidad que afecta a su herramienta de administración MySQL web, la cual de ser explotada, permitiría a un usuario no autorizado obtener el control completo de la base de datos. El informe contiene la respectiva mitigación de la vulnerabilidad.

Vulnerabilidad

CVE-2020-5504

Impacto

Esta vulnerabilidad permite a un usuario remoto ejecutar consultas SQL arbitrarias en la base de datos debido a una insuficiente sanitización de los datos entregados por el usuario en la página de cuentas de usuario. La explotación de esta vulnerabilidad permitiría a un usuario remoto leer, eliminar, insertar y modificar datos en la base de datos y obtener control completo de la aplicación en cuestión.

Productos Afectados

Todas las versiones de phpMyAdmin desde la 4.0.0 hasta la 4.9.3. También es vulnerable la versión 5.0.

Mitigación

Para las versiones 4.x, se debe actualizar a la versión 4.9.4 .

Para la versión 5.0, se debe actualizar a la versión 5.1.

Enlaces

<https://www.phpmyadmin.net/security/PMASA-2020-1/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5504>