Alerta de seguridad cibernética	9VSA20-00305-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2020
Última revisión	18 de octubre 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 Adobe respecto a vulnerabilidades que afectan a Magento Commerce y Magento Open Source. Un atacante podría aprovechar algunas de estas vulnerabilidades para tomar el control de un sistema afectado. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidad

CVE-2020-24407
CVE-2020-24400
CVE-2020-24402
CVE-2020-24408
CVE-2020-24401
CVE-2020-24404
CVE-2020-24405
CVE-2020-24403
CVE-2020-24406

Impactos

CVE-2020-24407
Esta vulnerabilidad, calificada como crítica, consiste en la omisión de lista de permisos de carga de archivos, lo que puede llevar a la ejecución de código arbitrario.

CVE-2020-24400
Esta vulnerabilidad, calificada como crítica, consiste en un error de inyección SQL pueden llevar a un acceso arbitrario a la base de datos de lectura o escritura.

CVE-2020-24402
Vulnerabilidad calificada como importante, consiste en la autorización incorrecta que podría permitir a un atacante la modificación no autorizada de la lista de clientes.

CVE-2020-24401
Vulnerabilidad calificada como importante, consiste en la invalidación insuficiente de la sesión del usuario que podría permitir a un atacante obtener acceso no autorizado a recursos restringidos.

CVE-2020-24404
Vulnerabilidad calificada como importante, consiste en la autorización incorrecta que podría permitir a un atacante la modificación no autorizada de las páginas de Magento CMS.

CVE-2020-24406
Vulnerabilidad calificada como moderada, consiste en la divulgación de información confidencial que podría permitir a un atacante la divulgación de la ruta raíz del documento.

CVE-2020-24408
Vulnerabilidad calificada como importante, consiste en la secuencia de comandos entre sitios (XSS almacenado), el que podría permitir a un atacante la ejecución arbitraria de JavaScript en el navegador.

CVE-2020-24405
Vulnerabilidad calificada como importante, consiste en la autorización incorrecta que podría permitir a un atacante obtener acceso no autorizado a recursos restringidos.

CVE-2020-24403
Vulnerabilidad calificada como importante, consiste en la autorización incorrecta que podría permitir a un atacante obtener acceso no autorizado a recursos restringidos.

Productos afectados

Las vulnerabilidades afectan a Magento Commerce y Magento Open Source, en las versiones anteriores a 2.4.1 y 2.3.6.

Mitigación

Con el objetivo de mitigar la vulnerabilidad, el fabricante recomienda actualizar los productos a las versiones 2.4.1 y 2.3.6, tanto para las versiones comerciales como open source.

Enlaces

https://helpx.adobe.com/security/products/magento/apsb20-59.html
https://devdocs.magento.com/guides/v2.4/release-notes/commerce-2-4-1.html
https://devdocs.magento.com/guides/v2.4/release-notes/open-source-2-4-1.html
https://devdocs.magento.com/guides/v2.3/release-notes/commerce-2-3-6.html
https://devdocs.magento.com/guides/v2.3/release-notes/open-source-2-3-6.html