

Alerta de seguridad cibernética	9VSA21-00362-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2021
Última revisión	13 de enero de 2021

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 entregada por Joomla sobre tres vulnerabilidades que afectan al gestor de contenidos.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-23123

CVE-2021-23124

CVE-2021-23125

Impacto

La falta de chequeos en la lista de control de acceso (ACL) en el endpoint “orderPosition” de “com_modules” expone nombres de módulos sin publicar o inaccesibles.

Productos afectados

Joomla! CMS desde la versión 3.0.0 hasta la 3.9.23.

Mitigación

La versión 3.9.24 mitiga la vulnerabilidad.

Enlaces

<https://developer.joomla.org/security-centre/836-20210101-core-com-modules-exposes-module-names.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23123>

Impacto

La falta de sanitización de datos en el atributo “aria-label” en “mod_breadcrumbs” permitiría a un atacante realizar ataques Cross-site Scripting (XSS).

Productos Afectados

Joomla! CMS desde la versión 3.9.0 hasta la 3.9.23.

Mitigación

La versión 3.9.24 mitiga la vulnerabilidad.

Enlaces

<https://developer.joomla.org/security-centre/837-20210102-core-xss-in-mod-breadcrumbs-aria-label-attribute.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23124>

Impacto

La falta de sanitización en parámetros relacionados a imágenes en múltiples vistas “com_tags” permitiría vectores de ataques Cross-site Scripting (XSS).

Productos afectados

Joomla! CMS desde la versión 3.1.0 hasta la 3.9.23.

Mitigación

La versión 3.9.24 mitiga la vulnerabilidad.

Enlaces

<https://developer.joomla.org/security-centre/838-20210103-core-xss-in-com-tags-image-parameters.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23125>