Alerta de seguridad cibernética	9VSA20-00278-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de julio de 2020
Última revisión	24 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 Joomla! respecto a seis vulnerabilidades que afectan al gestor de contenidos. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-15699
CVE-2020-15695
CVE-2020-15697
CVE-2020-15696
CVE-2020-15698
CWE-352 - [20200701]

CVE-2020-15699

La ausencia de chequeos de validación en el objeto “table usergroups” podría resultar en una configuración errada del sitio.

Productos Afectados
Gestor de contenidos Joomla! desde la versión 2.5.0 hasta la 3.9.19.

Mitigaciones
Actualizar a la versión 3.9.20 del CMS Joomla!.

Enlaces
https://developer.joomla.org/security-centre/819-20200702-core-missing-checks-can-lead-to-a-broken-usergroups-table-record.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15699

CVE-2020-15695

La ausencia del chequeo de token en la sección “remove request” de com_privacy permitiría a un atacante realizar ataques Cross Site Request Forgery (peticiones cruzadas entre sitios) en los sitios afectados.

Productos Afectados
Gestor de contenidos Joomla! desde la versión 3.9.0 hasta la 3.9.19.

Mitigaciones
Actualizar a la versión 3.9.20 del CMS Joomla!.

Enlaces
https://developer.joomla.org/security-centre/820-20200703-core-csrf-in-com-privacy-remove-request-feature.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15695

CVE-2020-15697

Campos internos de solo lectura en la clase “User table” podrían ser modificados por usuarios no autorizados.

Productos Afectados
Gestor de contenidos Joomla! desde la versión 3.9.0 hasta la 3.9.19.

Mitigaciones
Actualizar a la versión 3.9.20 del CMS Joomla!.

Enlaces
https://developer.joomla.org/security-centre/821-20200704-core-variable-tampering-via-user-table-class.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15697

CVE-2020-15696

La falta de filtro de datos ingresados en mod_random_image podría permitir a un atacante remoto realizar ataques XSS (Cross-site scripting) en el sitio afectado.

Productos Afectados
Gestor de contenidos Joomla! desde la versión 3.0.0 hasta la 3.9.19.

Mitigaciones
Actualizar a la versión 3.9.20 del CMS Joomla!.

Enlaces
https://developer.joomla.org/security-centre/822-20200705-core-escape-mod-random-image-link.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15696

CVE-2020-15698

La adecuada forma de filtrar en la pantalla de información de sistema podría exponer las credenciales de proxy o redis (almacén de datos en memoria).

Productos Afectados
Gestor de contenidos Joomla! desde la versión 3.0.0 hasta la 3.9.19.

Mitigaciones
Actualizar a la versión 3.9.20 del CMS Joomla!.

Enlaces
https://developer.joomla.org/security-centre/823-20200706-core-system-information-screen-could-expose-redis-or-proxy-credentials.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15698

CWE-352 - [20200701]

La ausencia del chequeo de token en el dispositivo final “com_installer” de ajax_install permitiría a un atacante realizar ataques Cross Site Request Forgery (peticiones cruzadas entre sitios) en los sitios afectados.

Productos Afectados
Gestor de contenidos Joomla! desde la versión 3.7 hasta la 3.9.19.

Mitigaciones
Actualizar a la versión 3.9.20 del CMS Joomla!.

Enlaces
https://developer.joomla.org/security-centre/818-20200701-core-csrf-in-com-installer-ajax-install-endpoint.html