Alerta de seguridad informática	9VSA20-00157-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de marzo de 2020
Última revisión	16 de marzo 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 entregada por Joomla! referente a vulnerabilidades que afectan al gestor de contenidos, las cuales de ser explotadas permitirían a un atacante realizar ataques Cross-site Scripting, Cross-site Request Forgery, inyecciones SQL, entre otros. Este informe incluye su respectiva mitigación.

Vulnerabilidades

CVE-2020-10241
CVE-2020-10242
CVE-2020-10238
CVE-2020-10239
CVE-2020-10240
CVE-2020-10243

Impactos

CVE-2020-10241
Debido a la insuficiente validación de la del origen petición HTTP en “com_templates” al procesar acciones de imagen. Un atacante remoto podría engañar a una víctima para que acceda a un sitio web especialmente diseñado y realizar peticiones maliciosas a otros sitios abiertos en el explorador de la víctima.

CVE-2020-10242
Debido a la insuficiente sanitización de datos ingresados por el usuario en los selectores CSS del Javascript “Protostar” y “Beez3”, un atacante remoto podría engañar a una víctima para que acceda a un sitio web especialmente diseñado, y ejecutar código HTML y JavaScript (XSS) arbitrario en el explorador de la víctima, amenazando con robar información potencialmente sensible, cambiar la apariencia de un sitio web y realizar ataques phishing.

CVE-2020-10238
Debido a restricciones de acceso incorrectas en “com_templates” un atacante remoto podría evadir las restricciones de seguridad implementadas y obtener acceso no autorizado a la aplicación.

CVE-2020-10239
Debido a restricciones de acceso incorrectas en el campo SQL “com_fields” un atacante remoto podría evadir las restricciones de seguridad implementadas y obtener acceso no autorizado a la aplicación.

CVE-2020-10240
Debido a la posible colisión de identificador en el componente “com_users” al no revisar la longitud de una entrada en la tabla usuario, un atacante podría evadir ciertas restricciones de seguridad y crear usuarios con nombres de usuario y email duplicados.

CVE-2020-10243
Debido a la insuficiente sanitización de datos ingresados por el usuario en el menú “Featured Articles”, un atacante remoto y autenticado podría enviar peticiones especialmente diseñadas a la aplicación afectada y ejecutar comandos SQL arbitrarios en la base de datos, permitiéndole leer, agregar, modificar y eliminar datos en la base de datos, comprometiéndola completamente.

Producto Afectado

Joomla! entre las versiones 1.7 hasta la 3.9.15.

Mitigación

Aplicar la actualización publicada por el fabricante siendo esta la versión 3.9.16 de Joomla!.

Enlaces

https://developer.joomla.org/security-centre/802-20200301-core-csrf-in-com-templates-image-actions.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10241
https://developer.joomla.org/security-centre/803-20200302-core-xss-in-protostar-and-beez3.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10242
https://developer.joomla.org/security-centre/804-20200303-core-incorrect-access-control-in-com-templates.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10238
https://developer.joomla.org/security-centre/806-20200305-core-incorrect-access-control-in-com-fields-sql-field.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10239
https://developer.joomla.org/security-centre/805-20200304-core-identifier-collisions-in-com-users.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10240
https://developer.joomla.org/security-centre/807-20200306-core-sql-injection-in-featured-articles-menu-parameters.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10243

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.16 11:10:58 -03'00'