BOLETÍN DE ALERTA

Boletín Nro.: 2020-07

Fecha de publicación: 18/03/2020

Tema: Actualización de seguridad para Joomla! aborda múltiples vulnerabilidades.

Las vulnerabilidades han sido identificadas como: CVE-2020-10243, CVE-2020-10242, CVE-2020-10241, CVE-2020-10240, CVE-2020-10239 y CVE-2020-10238.

Sistemas afectados:

- Joomla! desde las versiones 1.7 hasta la 3.9.15.

Descripción:

Recientemente Joomla! ha lanzado una actualización de seguridad donde informa la corrección de **seis** vulnerabilidades, las cuales de ser explotadas permitirían a un atacante realizar ataques **Cross-site Scripting, Cross-site Request Forgery e inyecciones SQL**. El CVE-2020-10243, se da debido a una validación incorrecta de los datos ingresados por el usuario en el menú **"Artículos destacados"**, esto permitiría a un atacante remoto autenticado enviar peticiones especialmente diseñadas y así ejecutar comandos SQL en la base de datos (leer, agregar, modificar y eliminar datos en la base de datos).

Por otro lado el CVE-2020-10242, se da debido a un manejo inadecuado en los selectores CSS del Javascript **"Protostar"** y **"Beez3"**. Esta vulnerabilidad, permitiría a un atacante remoto, realizar ataques **XSS**, con lo que se lograría manipular el navegador web de la víctima, cambiar la apariencia del sitio o redirigir a la víctima a sitios que contienen malware, entre otros.

Mientras que el CVE-2020-10241, se da debido a la falta de comprobación de token de imagen en **"com_templates"**. Esta falla da lugar a ataques del tipo **CSRF**, un atacante remoto podría diseñar solicitudes maliciosas y engañar a la víctima enviando esta solicitud, para que al momento de ejecutarla se inyecte en el sitio el código malicioso que pudiera contener la solicitud diseñada por el atacante. En otras palabras la explotación exitosa de esta vulnerabilidad permitiría la ejecución de código remoto en el sitio de la víctima.

En cuanto al CVE-2020-10240, se da debido a la falta de comprobación de longitud en la tabla de usuarios **"com_users"**, esto permite a un atacante que sea capaz de eludir las restricciones de seguridad, crear usuarios con nombres de usuario y correos electrónicos

duplicados.

El CVE-2020-10239, se da debido las restricciones de acceso inadecuadas en el campo **"com_fields"** de SQL, esto permitiría a un atacante remoto evadir las restricciones de seguridad implementadas y obtener acceso no autorizado a la aplicación.

Por último el CVE-2020-10238, se da debido a falta de comprobaciones **ACL** en **"com_templates",** esto permitiría a un atacante remoto obtener varios vectores de ataque potenciales.

Impacto:

La explotación exitosa de estas vulnerabilidades podrían dar lugar a ataques de tipo **XSS**, **CSRF**, **SQLi (Inyección SQL)**, además permitiría a un atacante crear usuarios con nombres de usuario y correos electrónicos duplicados, obtener acceso no autorizado a la aplicación y obtener varios vectores potenciales de ataque.

Solución y prevención:

- Se recomienda actualizar Joomla! a la versión 3.9.16, el cual la puede obtener desde el siguiente enlace.

Información adicional:

- https://developer.joomla.org/security-centre/807-20200306-core-sql-injection-in-featured-articles-menu-parameters.html
- https://developer.joomla.org/security-centre/803-20200302-core-xss-in-protostar-and-beez3.html
- https://developer.joomla.org/security-centre/802-20200301-core-csrf-in-com-templates-image-actions.html
- https://developer.joomla.org/security-centre/805-20200304-core-identifier-collisions-in-com-users.html
- https://developer.joomla.org/security-centre/806-20200305-core-incorrect-access-control-in-com-fields-sql-field.html
- https://developer.joomla.org/security-centre/804-20200303-core-incorrect-access-control-in-com-templates.html