Alerta de seguridad cibernética	9VSA20-00321-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de noviembre de 2020
Última revisión	18 de noviembre 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 Moodle respecto a múltiples vulnerabilidades que afectan al sistema de desarrollo de plataformas de aprendizaje. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-25627
CVE-2020-25628
CVE-2020-25629
CVE-2020-25630
CVE-2020-25631
CVE-2020-25698
CVE-2020-25699
CVE-2020-25700
CVE-2020-25701
CVE-2020-25702
CVE-2020-25703

CVE-2020-25627

Se sanitizó la entrada de datos en el parámetro “moodlenetprofile” en el perfil de usuario, ya que era posible realizar ataques Cross-site Scripting almacenados (Stored XSS). Esto permitía a un atacante comprometer completamente al sitio afectado. El impacto es “serio”.

Productos Afectados
La vulnerabilidad afecta a Moodle entre la versión 3.9 y la 3.9.1.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.9.2 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=410839
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25627

CVE-2020-25628

Se sanitizó la entrada de datos en la etiqueta “filtro” del gestor de etiquetas, ya que era posible realizar ataques Cross-site Scripting reflejados (Reflected XSS). Esto permitía a un atacante modificar la apariencia del sitio web, robar datos almacenados en el explorador, conducir a un usuario para descargar archivos maliciosos o hasta comprometer completamente al sitio afectado. El impacto es “serio”.

Productos Afectados
La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.1, 3.8 y la 3.8.4, 3.7 y la 3.7.7, 3.5 y la 3.5.13.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.9.2, 3.8.5, 3.7.8 y 3.5.14 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=410840
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25628

CVE-2020-25629

Usuarios con la opción de “conectarse como” en el contexto del curso (típicamente, gestores de curso) podrían obtener acceso a algunas de los sitios de administración al conectarse como “System manager”. El impacto es “menor”.

Productos Afectados
La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.1, 3.8 y la 3.8.4, 3.7 y la 3.7.7, 3.5 y la 3.5.13 y versiones anteriores sin soporte.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.9.2, 3.8.5, 3.7.8 y 3.5.14 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=410841
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25629

CVE-2020-25630

El tamaño descomprimido de los archivos ZIP no era comparado con la cuota de disponibilidad del usuario antes de realizar la descompresión, lo cual permitía un riesgo de denegación de servicios en el sistema afectado. El impacto es “serio”.

Productos Afectados
La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.1, 3.8 y la 3.8.4, 3.7 y la 3.7.7, 3.5 y la 3.5.13 y versiones anteriores sin soporte.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.9.2, 3.8.5, 3.7.8 y 3.5.14 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=410842
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25630

CVE-2020-25631

Era posible incluir código JavaScript en el título de un capítulo del libro, el cual no era manejado correctamente en la página “Add new chapter”. Nota: esta funcionalidad solo está disponible para usuarios confiables (como profesores), pero se incluyó como vulnerabilidad por precaución ya que no se sanitizaba correctamente en sitios con “Forceclean” habilitado.

Productos Afectados
La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.1, 3.8 y la 3.8.4, 3.7 y la 3.7.7.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.9.2, 3.8.5 y 3.7.8 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=410843
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25631

CVE-2020-25698

Las capacidades de enrolamiento de los usuarios no eran suficientemente validadas cuanto ellos recuperaban un curso existente, lo cual podría llevar a desenrolar a otros usuarios de cursos sin autorización de poder hacerlo.

Productos Afectados
La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.2, 3.8 y la 3.8.5, 3.7 y la 3.7.8, 3.5 y la 3.5.14 y versiones anteriores sin soporte.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.10, 3.9.3, 3.8.6, 3.7.9 y 3.5.15 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=413935
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25698

CVE-2020-25699

Insuficiente validaciones de capacidades podría permitir que usuarios que puedan restaurar un curso, pudiesen agregar nuevas capacidades al curso sin autorización.

Productos Afectados
La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.2, 3.8 y la 3.8.5, 3.7 y la 3.7.8, 3.5 y la 3.5.14 y versiones anteriores sin soporte.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.10, 3.9.3, 3.8.6, 3.7.9 y 3.5.15 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=413936
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25699

CVE-2020-25700

Por falta de validaciones, algunos servicios web de módulos de bases de datos permitían a estudiantes agregar entradas en grupos a los que ellos no permitían.

Productos Afectados
La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.2, 3.8 y la 3.8.5, 3.7 y la 3.7.8, 3.5 y la 3.5.14 y versiones anteriores sin soporte.

Mitigación
La vulnerabilidad fue mitigada en la versión 3.10, 3.9.3, 3.8.6, 3.7.9 y 3.5.15 de Moodle.

Enlaces
https://moodle.org/mod/forum/discuss.php?d=413938
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25700

CVE-2020-25701

Si la herramienta de subir curso era utilizada para eliminar un método de enrolamiento que no existía o no estaba habilitado, la herramienta podría equivocadamente habilitar ese método de enrolamiento. Esto podría permitir que usuarios no autorizados obtengan acceso al curso.

Productos Afectados

La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.2, 3.8 y la 3.8.5, 3.7 y la 3.7.8, 3.5 y la 3.5.14 y versiones anteriores sin soporte.

Mitigación

La vulnerabilidad fue mitigada en la versión 3.10, 3.9.3, 3.8.6, 3.7.9 y 3.5.15 de Moodle.

Enlaces

https://moodle.org/mod/forum/discuss.php?d=413939
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25701

CVE-2020-25702

Era posible incluir código JavaScript al renombrar “content bank items”, permitiendo un posible ataque Cross-site Scripting almacenado (Stored XSS).

Productos Afectados

La vulnerabilidad afecta a Moodle entre la versión 3.9 y la 3.9.2.

Mitigación

La vulnerabilidad fue mitigada en la versión 3.10 y 3.9.3 de Moodle.

Enlaces

https://moodle.org/mod/forum/discuss.php?d=413940
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25702

CVE-2020-25703

La descarga de la tabla de participantes siempre incluía correos de usuarios, aún cuando ellos habían configurado que su correo debía permanecer en oculto en la configuración “show user identity”.

Productos Afectados

La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.2, 3.8 y la 3.8.5, 3.7 y la 3.7.8.

Mitigación

La vulnerabilidad fue mitigada en la versión 3.10, 3.9.3, 3.8.6 y 3.7.9.

Enlaces

https://moodle.org/mod/forum/discuss.php?d=413941
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25703