Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2021-07

Fecha de publicación: 15/03/2021

Tema: Múltiples vulnerabilidades en Moodle

Versiones que se ven afectadas:

- de la 3.10 a la 3.10.1;
- de la 3.9 a la 3.9.4;
- de la 3.8 a la 3.8.7;
- de la 3.5 a la 3.5.16;
- versiones anteriores no soportadas.

Descripción

Moodle es una de las plataformas de aprendizaje un de las más utilizadas a nivel mundial y tal vez sea la más utilizada en nuestro país. Un equipo de seguridad ha detectado 7 vulnerabilidades, 2 de severidad crítica y 5 de severidad baja, que podrían permitir a un atacante realizar ataques de tipo XSS almacenado o SSRF ciego.

A continuación se describen las vulnerabilidades con sus respectivas severidad Crítica y Baja:

El CVE-2021-20279 severidad **crítica**, que afecta a las versiones 3.10 a 3.10.1, 3.9 a 3.9.4, 3.8 a 3.8.7, 3.5 a 3.5.16 y versiones anteriores no compatibles. Una validación o filtrado insuficientes en el campo para introducir el ID del usuario podría permitir a un usuario malintencionado realizar un ataque de tipo XSS almacenado (XSS stored).

El CVE-2021-20280 severidad **crítica**, que afecta a las versiones 3.10 a 3.10.1, 3.9 a 3.9.4, 3.8 a 3.8.7, 3.5 a 3.5.16 y versiones anteriores no compatibles. Un filtrado insuficiente en las respuestas de feedback podría permitir a un usuario malintencionado realizar un ataque de tipo XSS almacenado o SSRF ciego (blind).

El CVE-2021-20281 severidad **baja,** que afecta a las versiones 3.10 a 3.10.1, 3.9 a 3.9.4, 3.8 a 3.8.7, 3.5 a 3.5.16 y versiones anteriores no compatibles. Esta vulnerabilidad podría permitir a un atacante sin privilegios ver los nombres completos de otros usuarios a través del online users block.

El CVE-2021-20282 severidad **baja,** que afecta a las versiones 3.10 a 3.10.1, 3.9 a 3.9.4, 3.8 a 3.8.7, 3.5 a 3.5.16 y versiones anteriores no compatibles. Esta vulnerabilidad permite a un atacante hacerse con el control de la cuenta de la víctima. Sucede cuando este último crea una cuenta de usuario, donde el atacante puede verificar la cuenta sin tener acceso al enlace secreto de verificación.

El CVE-2021-20283 severidad **baja,** que afecta a las versiones 3.10 a 3.10.1, 3.9 a 3.9.4, 3.8 a 3.8.7, 3.5 a 3.5.16 y versiones anteriores no compatibles. Esta vulnerabilidad afecta al servicio web responsable de obtener los cursos inscritos por un usuario y no verifica el acceso al perfil en cada curso.

El CVE-2021-20284 severidad **baja**, que afecta a las versiones 3.10 a 3.10.1, 3.9 a 3.9.4, 3.8 a 3.8.7, 3.5 a 3.5.16 y versiones anteriores no compatibles. La versión de JQuery utilizada por Moodle requería actualizarse a 3.5.1 para parchear algunas vulnerabilidades potenciales publicadas.

Impacto:

La explotación exitosa de las vulnerabilidades críticas citadas pueden derivar en el control total de las cuentas de usuarios de la plataforma Moodle, así como también la inyección de código malicioso en la plataforma, afectando a todos los visitantes de la misma. .

Solución y mitigación

- Actualice a la última versión, en función de la versión afectada:
  - De 3.10 a la 3.10.1 actualizar a 3.10.2
  - De 3.9 a la 3.9.4 actualizar a 3.9.5
  - De 3.8 a la 3.8.7 actualizar a 3.8.8
  - De 3.5 a la 3.5.16 atualizar a 3.5.17
- Además compartimos una guía elaborada por terceros que le puede ayuda actualizar su versión de moodle https://www.evirtualplus.com/como-actualizar-moodle-la-guia/

Referencias

- https://moodle.org/mod/forum/discuss.php?d=419650
- https://moodle.org/mod/forum/discuss.php?d=419651
- https://moodle.org/mod/forum/discuss.php?d=419652
- https://moodle.org/mod/forum/discuss.php?d=419653
- https://moodle.org/mod/forum/discuss.php?d=419654
- https://moodle.org/mod/forum/discuss.php?d=419655
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-moodle-13
- https://www.evirtualplus.com/como-actualizar-moodle-la-guia/