Investigadores de seguridad cibernética descubrieron vulnerabilidades en algunos complementos populares del sistema de gestión de aprendizaje en línea (LMS), que distintas organizaciones y universidades utilizan para ofrecer cursos de capacitación en línea por medio de sus sitios web basados en WordPress.

Según el equipo de investigación de Check Point, los tres plugins de WordPress en cuestión, LearnPress, LearnDash y LifterLMS, tienen vulnerabilidades de seguridad que podrían permitir a los estudiantes, además de usuarios no autenticados, acceso a la información personal de los usuarios registrados e incluso, alcanzar privilegios de maestros.

> *«Debido al coronavirus, estamos haciendo todo desde nuestros hogares, incluido nuestro aprendizaje formal. Las vulnerabilidades encontradas permiten a los estudiantes, y aveces incluso a usuarios no autenticados, obtener información confidencial o tomar el control de las plataformas LMS»,* dijo Omri Herscovici, de Check Point.

Los tres sistemas LMS se instalan en aproximadamente 100 mil plataformas educativas diferentes, incluidas las principales universidades como la Universidad de Florida, la Universidad de Michigan y la Universidad de Washington, entre otras.

Los LMS facilitan el aprendizaje en línea a través de una aplicación de software que permite a las instituciones académicas y a los empleadores crear el currículo del curso, compartir el trabajo del curso, inscribir estudiantes y evaluarlos con cuestionarios.

Los complementos como LearnPress, LearnDash y LifterLMS facilitan la adaptación de cualquier sitio de WordPress a un LMS totalmente funcional y fácil de utilizar.

Las vulnerabilidades en LearnPress comienzan desde la inyección SQL ciega (CVE-2020-6010) hasta la escalada de privilegios (CVE-2020-11511), que puede autorizar a un usuario existente a obtener el rol de maestro.

> *«Inesperadamente, el código no verifica los permisos del usuario solicitante, por lo tanto, permite que cualquier estudiante llame a esta función»*, dijeron los investigadores.

Por otro lado, LearnDash tiene una falla de inyección de SQL (CVE-2020-6009), que permite a un adversario elaborar una consulta SQL maliciosa utilizando el simulador de servicio de mensajes de notificación de pago instantáneo (IPN) de PayPal para activar transacciones de inscripción en cursos falsos.

Finalmente, la vulnerabilidad de escritura arbitraria de archivos de LifterLMS (CVE-2020-6008), explota la naturaleza dinámica de las aplicaciones PHP para permitir que un atacante, por ejemplo, un estudiante registrado en un curso específico, cambie su nombre de perfil a una pieza maliciosa de código PHP.

Las vulnerabilidades hacen posible que los hackers roben información personal, como nombres, correos electrónicos, nombres de usuario, contraseñas, etcétera, y que los estudiantes cambien las calificaciones, recuperen exámenes y respondan las pruebas de antemano, además de falsificar certificados.

> *«Las plataformas implican pagos, por lo tanto, los esquemas financieros también son aplicables en el caso de modificar el sitio web sin la información del webmaster»,* advierten los investigadores.

Check Point Research asegura que las vulnerabilidad se descubrieron en marzo y se divulgaron de forma responsable a las plataformas en cuestión. Desde entonces, los tres sistemas LMS ya lanzaron parches para abordar los problemas.