Si utilizas OXID eShop para su sitio web de comercio electrónico, debes actualizarlo inmediatamente para evitar que tu sitio se vea comprometido.

Investigadores de seguridad cibernética descubrieron dos vulnerabilidades críticas en el software de comercio electrónico que podrían permitir a los hackers no autenticados tomar el control total de los sitios web de comercio electrónico vulnerables de forma remota en pocos segundos.

OXID eShop es una de las principales soluciones de software para tiendas de comercio electrónico alemanas, su edición empresarial se utiliza por líderes en la industria, como Mercedes, BitButguer y Edeka.

Los investigadores de RIPS Technologies GmbH compartieron sus últimos hallazgos, detallando dos vulnerabilidades críticas de seguridad que afectan a las últimas versiones en las ediciones Enterprise, Professional y Community de OXID eShop.

Es importante mencionar que no se requiere ninguna interacción entre el atacante y la víctima para ejecutar ambas vulnerabilidades, y las fallas funcionan en contra de la configuración predeterminada del software de comercio electrónico.

Falla de inyección SQL

La primera vulnerabilidad, asignada como CVE-2019-13026, es una vulnerabilidad de inyección SQL que permite a un atacante no autenticado simplemente crear una nueva cuenta de administrador, con una contraseña de su elección, en un sitio web que ejecuta cualquier versión vulnerable de OXID.

> *«Una inyección SQL no autenticada puede explotarse al ver los detalles de un producto. Debido a que la base de datos subyacente utiliza el controlador de la base de datos PDO, las consultas apiladas se pueden utilizar para INSERTAR datos en la base de datos. En nuestro exploit abusamos de estos para INSERTAR un nuevo*

> *usuario administrador»,* dijeron los investigadores a The Hacker News.

El siguiente video es una prueba de concepto compartida por los investigadores de seguridad:

Aunque el sistema de base de datos PDO ha sido diseñado para evitar ataques de inyección SQL utilizando sentencias preparadas, el uso de comandos SQL de compilación dinámica podría dejar consultas apiladas con mayor riesgo de contaminarse.

Falla de ejecución remota de código

La segunda vulnerabilidad es un problema de inyección de objetos PHP, que reside en el panel de administración del software OXID eSHop y ocurre cuando la entrada suministrada por el usuario no se desinfecta correctamente antes de pasar a la función PHP unserialize().

Esta vulnerabilidad se puede aprovechar para obtener la ejecución remota de código en el servidor, sin embargo, requiere acceso administrativo que se puede obtener utilizando la primera vulnerabilidad.

> *«Luego se puede encadenar una segunda vulnerabilidad para obtener la ejecución remota de código en el servidor. Tenemos un exploit Python 2.7 totalmente funcional que puede comprometer directamente a los OXID eShops que requieren solo la URL como argumento»,* agregaron los investigadores.

Video demostrativos del ataque RCE:

Al tener éxito, los hackers pueden ejecutar de forma remota código malicioso en el servidor subyacente, o instalar su propio complemento malicioso para robar las tarjetas de crédito de los usuarios, la información de la cuenta de PayPal y cualquier información financiera altamente sensible que pase por el sistema eShop, al igual que los ataques de MageCart.

Los investigadores de RIPS informaron sus hallazgos a OXID y la compañía reconoció el problema, luego lanzó OXID eShop v6.0.5 y 6.1.4 para las tres ediciones.

Parece que la compañía no parchó la segunda vulnerabilidad, solo la mitigó abordando el primer problema. Sin embargo, en el futuro, si se descubre algún problema de toma de control del administrador, se volverán a ver los ataques RCE.