VMware está instando a los usuarios a desinstalar el Plugin de Autenticación Mejorada (EAP), que ha sido marcado como obsoleto, después de descubrir una seria vulnerabilidad de seguridad.

Identificado como CVE-2024-22245 (puntuación CVSS: 9.6), el defecto ha sido descrito como un fallo arbitrario en el relevo de autenticación.

> *«Un actor malicioso podría engañar a un usuario del dominio objetivo con EAP instalado en su navegador web para solicitar y transmitir tickets de servicio para Nombres Principales de Servicio (SPNs) arbitrarios de Active Directory»,* indicó la compañía en un aviso.

EAP, considerado obsoleto desde marzo de 2021, es un paquete de software diseñado para permitir el acceso directo a las interfaces y herramientas de gestión de vSphere a través de un navegador web. No se incluye por defecto y no forma parte de vCenter Server, ESXi o Cloud Foundation.

En la misma herramienta, también se ha descubierto una vulnerabilidad de secuestro de sesión (CVE-2024-22250, puntuación CVSS: 7.8) que podría permitir a un actor malicioso con acceso local no privilegiado a un sistema operativo Windows apoderarse de una sesión privilegiada de EAP.

Ceri Coburn de Pen Test Partners ha sido reconocido por descubrir y reportar ambas vulnerabilidades.

Es importante señalar que estas deficiencias solo afectan a los usuarios que han añadido EAP a sistemas Microsoft Windows para conectarse a VMware vSphere a través del Cliente vSphere.

La empresa, propiedad de Broadcom, anunció que no abordará las vulnerabilidades, en su lugar, recomienda a los usuarios eliminar completamente el plugin para mitigar posibles

amenazas.

> *«El Plugin de Autenticación Mejorada puede desinstalarse de los sistemas cliente utilizando el método de desinstalación de software del sistema operativo cliente»,* añadió.

Este anuncio coincide con la revelación de múltiples fallos de scripting entre sitios (XSS) por parte de SonarSource, que afectan al sistema de gestión de contenidos Joomla! (CVE-2024-21726). Estos problemas han sido abordados en las versiones 5.0.3 y 4.4.3.

> *«La filtración de contenido insuficiente conduce a vulnerabilidades XSS en varios componentes»*, afirmó Joomla! en su propio aviso, calificando la vulnerabilidad como moderada en gravedad.
>
> *«Los atacantes pueden aprovechar el problema para lograr la ejecución remota de código al engañar a un administrador para que haga clic en un enlace malicioso»,* explicó el investigador de seguridad Stefan Schiller. Detalles técnicos adicionales sobre la falla se han retenido por el momento.

En un desarrollo relacionado, se han identificado varias vulnerabilidades y configuraciones incorrectas de alta y crítica gravedad en el lenguaje de programación Apex desarrollado por Salesforce para construir aplicaciones empresariales.

En el centro del problema está la capacidad de ejecutar código Apex en modo *«sin compartir»*, lo cual omite los permisos de un usuario, permitiendo que actores maliciosos lean o extraigan datos e incluso proporcionen entradas especialmente diseñadas para alterar el flujo de ejecución.

> *«Si se explotan, estas vulnerabilidades pueden provocar la fuga de datos, la corrupción de datos y daños a las funciones comerciales en Salesforce»*, advirtió el investigador de seguridad Nitay Bachrach de Varonix.