GitHub ha lanzado soluciones para corregir una vulnerabilidad crítica en GitHub Enterprise Server (GHES) que podría permitir a un atacante evitar las protecciones de autenticación.

Identificada como CVE-2024-4985 (con una puntuación CVSS de 10.0), esta vulnerabilidad podría permitir el acceso no autorizado a una instancia sin necesidad de autenticación previa.

> *«En instancias que utilizan la autenticación de inicio de sesión único (SSO) de SAML con la característica opcional de afirmaciones cifradas, un atacante podría falsificar una respuesta SAML para obtener acceso y/o provisionar un usuario con privilegios de administrador»*, señaló la compañía en un aviso.

GHES es una plataforma autoalojada para el desarrollo de software que permite a las organizaciones almacenar y desarrollar software utilizando el control de versiones Git, así como automatizar la canalización de despliegue.

El problema afecta a todas las versiones de GHES anteriores a la 3.13.0 y se ha solucionado en las versiones 3.9.15, 3.10.12, 3.11.10 y 3.12.4.

GitHub también destacó que las afirmaciones cifradas no están habilitadas por defecto y que la vulnerabilidad no afecta a las instancias que no utilizan SAML SSO o aquellas que utilizan SAML SSO sin afirmaciones cifradas.

Las afirmaciones cifradas permiten a los administradores del sitio mejorar la seguridad de una instancia de GHES con SAML SSO cifrando los mensajes que el proveedor de identidad SAML (IdP) envía durante el proceso de autenticación.

Se recomienda a las organizaciones que usen una versión vulnerable de GHES que actualicen a la última versión para protegerse contra posibles amenazas de seguridad.