



GitHub corrige vulnerabilidad crítica de Enterprise Server que permite el acceso no autorizado a instancias

GitHub ha publicado [actualizaciones](#) de seguridad para Enterprise Server (GHES) con el fin de corregir varios problemas, incluyendo un error crítico que podría permitir el acceso no autorizado a una instancia.

La vulnerabilidad, denominada CVE-2024-9487, tiene una puntuación CVS de 9.5 sobre 10.

«Un atacante podría evitar la autenticación de inicio de sesión único (SSO) de SAML utilizando la función opcional de afirmaciones cifradas, lo que permitiría la creación no autorizada de usuarios y acceso a la instancia, al aprovechar una vulnerabilidad en la verificación incorrecta de firmas criptográficas en GitHub Enterprise Server», [advirtió GitHub](#) en un comunicado.

La compañía, propiedad de Microsoft, describió la falla como una regresión que surgió durante los arreglos posteriores a la vulnerabilidad CVE-2024-4985 (puntuación CVSS: 10.0), un error de máxima gravedad que fue solucionado en mayo de 2024.

GitHub también corrigió otros dos problemas adicionales:

- CVE-2024-9539 (puntuación CVSS: 5.7): una vulnerabilidad de divulgación de información que podría permitir a un atacante acceder a los metadatos de un usuario víctima al hacer clic en enlaces maliciosos para activos SVG.
- Exposición de datos sensibles en formularios HTML en la consola de administración (sin número CVE asignado).

Estas tres vulnerabilidades de seguridad han sido corregidas en las versiones de Enterprise Server 3.14.2, 3.13.5, 3.12.10 y 3.11.16.

En agosto, GitHub también solucionó una falla crítica de seguridad (CVE-2024-6800, puntuación CVSS: 9.5) que podría ser explotada para obtener privilegios de administrador del sitio.



GitHub corrige vulnerabilidad crítica de Enterprise Server que permite el acceso no autorizado a instancias

Se recomienda encarecidamente a las organizaciones que utilicen una versión vulnerable y autoalojada de GHES que actualicen a la última versión para protegerse de posibles riesgos de seguridad.