GitLab ha lanzado actualizaciones para corregir una vulnerabilidad crítica que afecta tanto a la Edición Comunitaria (CE) como a la Edición Empresarial (EE), la cual podría permitir una omisión de autenticación.

La falla está vinculada a la biblioteca ruby-saml (CVE-2024-45409, con una calificación CVSS de 10.0), y podría permitir a un atacante acceder al sistema vulnerable como un usuario arbitrario. Los desarrolladores de la biblioteca solucionaron el problema la semana pasada.

El fallo se debe a que la biblioteca no valida correctamente la firma de la Respuesta SAML. SAML, o Lenguaje de Marcado de Aserciones de Seguridad, es un protocolo que facilita el inicio de sesión único (SSO) y el intercambio de datos de autenticación y autorización entre aplicaciones y sitios web.

> *«Un atacante sin autenticación que tenga acceso a cualquier documento SAML firmado por el proveedor de identidad (IdP) puede manipular una Respuesta SAML/Aserción con contenido arbitrario. Esto le permitiría al atacante iniciar sesión como cualquier usuario en el sistema vulnerable»,* según un comunicado de seguridad.

Además, esta vulnerabilidad también afecta a omniauth-saml, que lanzó su propia actualización (versión 2.2.1) para actualizar ruby-saml a la versión 1.17.

El último parche de GitLab actualiza las dependencias de omniauth-saml a la versión 2.2.1 y ruby-saml a la versión 1.17.0. Este parche incluye las versiones 17.3.3, 17.2.7, 17.1.8, 17.0.8 y 16.11.10.

Como medida preventiva, GitLab recomienda a los usuarios con instalaciones autogestionadas activar la autenticación de dos factores (2FA) para todas las cuentas y deshabilitar la opción que permite omitir el segundo factor en SAML.

GitLab no ha informado de casos conocidos de explotación activa de esta vulnerabilidad,

pero ha compartido indicadores de intentos o posibles explotaciones exitosas, lo que sugiere que actores maliciosos podrían estar intentando aprovechar la debilidad para acceder a instancias vulnerables de GitLab.

> *«Los intentos de explotación exitosos generarán eventos en los registros relacionados con SAML. Un intento exitoso registrará el valor extern_id configurado por el atacante»,* señaló GitLab.
>
> *«Los intentos fallidos podrían generar un ValidationError desde la biblioteca RubySaml, lo que puede ocurrir por diversas razones relacionadas con la complejidad de crear un exploit funcional».*

Este anuncio coincide con la inclusión de cinco fallos de seguridad en el catálogo de Vulnerabilidades Explotadas Conocidas (KEV) de la Agencia de Seguridad de Infraestructura y Ciberseguridad de los EE. UU. (CISA). Entre ellos se encuentra un error crítico recientemente reportado que afecta a Apache HugeGraph-Server (CVE-2024-27348, con una calificación CVSS de 9.8), basado en pruebas de explotación activa.

Las agencias de la Rama Ejecutiva Civil Federal (FCEB) han sido instadas a corregir las vulnerabilidades identificadas antes del 9 de octubre de 2024 para proteger sus redes frente a amenazas activas.