Basque CyberSecurity Centre

Vulnerabilidad crítica en GitLab Community Edition (CE) y Enterprise Edition (EE)

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

GitLab ha publicado una actualización de seguridad en la que se aborda una vulnerabilidad, cuya severidad ha sido calificada como crítica, y que afecta a la aplicación de código abierto utilizada para alojar repositorios Git, conocida como GitLab Community Edition (CE). De igual manera, GitLab Enterprise Edition (EE), una plataforma de programación dirigida al desarrollo y ejecución software de aplicaciones escritas en Java, es vulnerable ante el error destacado.

La vulnerabilidad, identificada bajo el CVE-2023-2825, de momento no tiene asignada una puntuación de acuerdo a la escala CVSSv3 según el NIST, pero ha sido calificada por el fabricante como crítica. Cabe destacar que, por el momento, no se tiene el conocimiento de que el fallo se esté explotando de manera activa en la red.

Dicho error, reportado por parte del investigador *pwnie* puede resultar en una lectura de archivos localizados en el servidor. En base a las graves repercusiones que puede suponer la explotación de la vulnerabilidad destacada, la solución radica en seguir las instrucciones de mitigación proporcionadas por parte de GitLab.

El fabricante ya ha publicado el parche correspondiente, corrigiendo de esta manera el fallo crítico destacado, por lo que, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Análisis técnico

La vulnerabilidad destacada, identificada bajo el CVE-2023-2825, afecta tanto a GitLab Community Edition (CE) como a GitLab Enterprise Edition (EE). Más específicamente, el error mencionado permite un atacante remoto ejecutar ataques de traspaso de directorios. La vulnerabilidad existe debido a un error en la validación de entrada en el caso de que exista un archivo adjunto en un proyecto accesible de manera pública, y que se encuentra disponible en al menos cinco grupos distintos. En el caso de que un actor de amenazas lleve a cabo su correcta explotación, podrá llevar a cabo una lectura de los archivos ubicados en el servidor.

Las métricas de evaluación de la vulnerabilidad anteriormente descrita se componen de:

CVSS Base: 10.0

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

Finalmente, los productos afectados por la anterior vulnerabilidad son los siguientes:

- GitLab Community Edition (CE) versión 16.0.0.
- GitLab Enterprise Edition (EE) versión 16.0.0.

3. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Es extremadamente importante que se tomen medidas rápidamente para solucionar el error destacado. Por ello, dada la gravedad de la vulnerabilidad, se recomienda aplicar las actualizaciones proporcionadas por la compañía actualizando GitLab Community Edition (CE) y GitLab Enterprise Edition (EE) a la versión 16.0.1.

Las actualizaciones mencionadas pueden encontrarse a través del siguiente enlace:

- https://about.gitlab.com/update/

Debido a que se trata de una vulnerabilidad cuya severidad es crítica, el equipo de GitLab recomienda encarecidamente a los usuarios que lleven a cabo lo antes posibles la actualización correspondiente de dichos productos.

4. Referencias Adicionales

- GitLab.
- GitLab Critical Security Release: 16.0.1.
- GitLab Community Edition (CE).
- GitLab Enterprise Edition (EE).
- Java.
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').
- CWE-20: Improper Input Validation.
- Update GitLab.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA