BOLETÍN DE ALERTA

Boletín Nro.: 2023-26
Fecha de publicación: 25/05/2023

Tema: Vulnerabilidad de lectura arbitraria de archivos en productos GitLab.

Las versiones afectadas son:

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

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a GitLab Community Edition (*CE*) y Enterprise Edition (*EE*), que permitiría a un atacante realizar lectura arbitraria de archivos en el servidor afectado.

La vulnerabilidad identificada como CVE-2023-2825, de severidad "Crítica", con puntuación asignada de 10.0. Esta vulnerabilidad del tipo *path traversal* se debe a un error de acceso cuando un archivo se encuentra adjunto en un proyecto público anidado dentro de al menos 5 grupos en GitLab Community Edition (*CE*) y Enterprise Edition (*EE*). Esto permitiría a un atacante no autenticado a través de ataques del tipo *path traversal*, leer archivos arbitrarios en el servidor afectado.

Cabe mencionar que cuando no se menciona ningún tipo específico de implementación de un producto (*omnibus, source code, helm chart, etc*.), significa que todos los tipos se ven afectados.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado realizar lectura arbitraria de archivos en el servidor afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante en el siguiente enlace:

- GitLab Community Edition (CE) and Enterprise Edition (EE) 16.0.1

Así también, tener en cuenta las mejores prácticas para la protección de cada instancia de GitLab detalladas a continuación:

1. Controles de visibilidad y acceso: Definir el acceso de los usuarios autorizados a la instancia en *Área de administración > Configuración > Configuración general:* "*controles de visibilidad y acceso*"
- Permitir la utilización de las claves RSA SSH, así como ED25519.
- Utilizar la autenticación SSH sin contraseña en lugar de la autenticación con contraseña.

Para obtener más información acerca de las restricciones sobre las claves SSH, ir al siguiente enlace.

2. Definir restricciones a los usuarios en cada instancia en *Área de administración > Configuración > Configuración general:*

2.1 Restricción de registro:

- Verificar que el registro abierto (*open sign-up*) se encuentre deshabitado en la instancia.
- Verificar que la opción "*Enviar correo electrónico de confirmación al registrarse*" esté marcada.
- Si se desea restringir el acceso a un subgrupo de usuarios de la organización, considerar la utilización de la configuración de una lista blanca para el dominio de la organización (por ejemplo, "*example.com*") que les permita registrarse.
- Considerar utilizar una contraseña con longitud mínima de 12 caracteres, principalmente para los usuarios que tengan acceso a la instancia. Para más información aquí.

Para obtener más información acerca de la restricción de registros, ir al siguiente enlace.

2.2 Restricción de inicio de sesión:

- Verificar que la autenticación de doble factor (*2FA*) se encuentre habilitada.
- En caso de no contar con Autenticación multifactor (MFA), deshabilitar "*autenticación de contraseña habilitada para Git sobre HTTP (S)*".

Para obtener más información acerca de la restricción de inicio de sesión, ir al siguiente enlace.

2.3 Visibilidad y privacidad:

- Verificar que la visibilidad del proyecto esté establecida en "*privada*", en los proyectos existentes y los proyectos nuevos. Para más información aquí.

3. Rendimiento y ajustes de red: proteger el uso de la red en *Área de administración > Red > Límites de velocidad de usuario e IP:*

- "*Habilitar límite de velocidad de solicitudes no autenticadas*"
- "*Habilitar el límite de velocidad de solicitud de API autenticada*"
- "Habilitar límite de velocidad de solicitudes web autenticadas"

Para obtener más información acerca de límites de velocidad de usuario e IP, ir al siguiente enlace.

4. Webhooks: restricción de servicios accesibles públicamente en *Área de administración > Red > Solicitudes salientes:*

- Si bien la opción "*permitir solicitudes a la red local desde enlaces web y servicios*" está deshabilitada de manera predeterminada, también se debe desmarcar la opción "*permitir solicitudes a la red local desde enlaces del sistema*".

Para obtener más información acerca de Webhooks, ir al siguiente enlace.

5. Rutas protegidas en *Área de administración > Red > Rutas protegidas:*

- Verificar que se encuentre marcado "*Habilitar límite de velocidad de rutas protegidas*".

Para obtener más información acerca de ruta protegidas, ir al siguiente enlace.

Para más detalle sobre las mejores prácticas visitar el siguiente enlace.

Información adicional:

- https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2825
- https://about.gitlab.com/update/
- https://about.gitlab.com/blog/2020/05/20/gitlab-instance-security-best-practices/