



## **BOLETÍN DE ALERTA**

**Boletín Nro.:** 2021-08

**Fecha de publicación:** 30/03/2021

**Tema:** Vulnerabilidad RCE en GitLab CE/EE

### **Versiones que se ven afectadas:**

- GitLab CE/EE versión 13.2 y posteriores

### **Descripción**

Se ha detectado una vulnerabilidad en GitLab CE/EE catalogada como [CVE-2021-22192](#) de severidad **crítica** puntuación **9,9** que afecta a todas las versiones gitlab a partir de 13.2 en adelante que permite a un atacante ejecutar código arbitrario en el servidor afectado sin necesidad de estar autenticado. No se publicaron mayores detalles sobre la vulnerabilidad, la cual fue reportada de manera privada a los desarrolladores de GitLab.

GitLab es una solución de control de versiones y desarrollo de software colaborativo basado en Git, que también tiene una versión Cloud, como servicio, mantenida por el equipo de Gitlab y no está afectada por la vulnerabilidad; sin embargo, muchas organizaciones utilizan su propio servidor de gestión de proyectos de software mediante una instalación on-premise de Gitlab. Dichas organizaciones deben actualizar cuanto antes el software.

GitLab ha publicado el parche de emergencia 13.9.3 el cual corrige dicha vulnerabilidad. Además, seguidamente, ha publicado la versión 13.10 la cual además incluye otras mejoras.

### **Impacto:**

La explotación de esta vulnerabilidad permite que cualquier atacante remoto no autenticado ejecute código arbitrario, logrando el control completo del servidor.

### **Solución y mitigación**

- Actualizar a la última versión lo más antes posible.
  - Para actualizar GitLab, consulte la [página Actualizar](#).
  - Para actualizar Gitlab Runner, consulte la [página Actualización de Runner](#).



Ministerio de  
**TECNOLOGÍAS  
DE LA INFORMACIÓN  
Y COMUNICACIÓN**



**TETÃ REKUÁI  
GOBIERNO NACIONAL**

## Referencias

- <https://about.gitlab.com/releases/2021/03/17/security-release-gitlab-13-9-4-released/#remote-code-execution-via-unsafe-user-controlled-markdown-rendering-options>
- <https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2021-22192>
- <https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22192.json>