

Boletín de alerta

Boletín Nro.: 118

Fecha de publicación: 21/10/2026

Tema: Alerta 2026-118 Vulnerabilidad crítica en GitLab permite RCE sin autenticación

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta tanto GitLab CE como GitLab EE. GitLab publicó correcciones en siete ramas, incluidas cuatro anteriores a su ventana habitual de mantenimiento.

Producto	Versiones afectadas	Versión corregida
GitLab CE / EE	Desde 7.0 hasta versiones anteriores a 18.11.13	18.11.13
GitLab CE / EE	19.0.x anteriores a 19.0.10	19.0.10
GitLab CE / EE	19.1.x anteriores a 19.1.9	19.1.9
GitLab CE / EE	19.2.x anteriores a 19.2.9	19.2.9
GitLab CE / EE	19.3.x anteriores a 19.3.6	19.3.6
GitLab CE / EE	19.4.x anteriores a 19.4.3	19.4.3
GitLab CE / EE	19.5.x anteriores a 19.5.1	19.5.1

Descripción

Se ha publicado una vulnerabilidad de severidad máxima que (CVSSv3.1 10 – CRITICO) en GitLab, bajo determinadas condiciones, permite a un atacante sin autenticación ejecutar código arbitrario en el servidor, la misma ha sido etiquetada como CVE-2026-110264.

La falla afecta GitLab Community Edition —CE— y Enterprise Edition —EE— desde la versión 7.0 y se origina en un desbordamiento de enteros durante la compilación de expresiones regulares especialmente manipuladas. Las organizaciones con instalaciones autogestionadas deben actualizar de inmediato, incluso si aplicaron los parches publicados el 12 de octubre, ya que estos no corrigen esta nueva vulnerabilidad.

El problema afecta al compilador de expresiones regulares utilizado por GitLab. Una expresión especialmente diseñada puede desencadenar un desbordamiento de enteros y, bajo ciertas condiciones, permitir ejecución de código en el servidor sin credenciales ni interacción del usuario.

GitLab no ha divulgado todas las condiciones necesarias para alcanzar el componente vulnerable. Por ello, no es posible descartar la exposición únicamente por la configuración de la instancia. El aviso no ofrece una mitigación temporal que sustituya la actualización.

Solución

La solución consiste en actualizar cada instancia afectada a una de las versiones corregidas de su rama o a una versión posterior que incluya la corrección, siguiendo la ruta de actualización admitida por GitLab. Se debe priorizar las instancias expuestas a Internet, sin excluir los servidores internos. Los parches del 12 de octubre para CVE-2026-97229 no corrigen CVE-2026-110264; las instalaciones actualizadas en esa fecha deben revisarse nuevamente.

Para info sobre como actualizar, visita el siguiente enlace:

<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released>

Información adicional:

- GitLab — aviso oficial y versiones corregidas:
<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>
- The Hacker News — análisis de la vulnerabilidad y alcance:
<https://thehackernews.com/2026/10/critical-gitlab-flaw-cvss-100-could.html>