GitLab publicó el 21 de octubre una serie de correcciones para solucionar una vulnerabilidad que permite a un atacante ejecutar código en un servidor autogestionado sin necesidad de iniciar sesión. El problema afecta a todas las versiones del software desde la 7.0, lanzada en 2014.

La actualización también resulta importante para los administradores que instalaron un parche nueve días antes. La actualización del 12 de octubre solo abarcaba las versiones 19.2 y posteriores, mientras que las nuevas versiones corregidas corresponden a una revisión adicional. Por ello, las instalaciones que se actualizaron en aquella fecha vuelven a estar expuestas si no aplican la nueva corrección.

La vulnerabilidad, identificada como CVE-2026-110264, obtuvo una puntuación de 10.0 en la escala CVSS, el valor máximo posible. GitLab explica que, bajo determinadas circunstancias, un usuario no autenticado podría ejecutar código arbitrario en el servidor debido a un desbordamiento de enteros durante la compilación de una expresión regular diseñada de forma maliciosa.

Hasta el momento, GitLab no ha especificado cuáles son las condiciones necesarias para que se produzca este fallo. La empresa tampoco ha detectado indicios de que la vulnerabilidad se haya utilizado en ataques. Además, al 22 de octubre, el problema no figuraba en el catálogo de vulnerabilidades explotadas conocidas de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de Estados Unidos (CISA).

Las medidas correctivas solo son necesarias para las instalaciones autogestionadas. GitLab.com ya opera con una versión que incluye la solución, mientras que los clientes de GitLab Dedicated que utilizan las versiones internas 19.3.5-internal0 y 19.4.2-internal0, o posteriores, también cuentan con la protección correspondiente.

GitLab solucionó la vulnerabilidad mediante la publicación simultánea de siete versiones corregidas.

Si corres	Actualizar a

19.5 antes de 19.5.1	19.5.1
19.4 antes de 19.4.3	19.4.3
19.3 antes de 19.3.6	19.3.6
19.2 antes de 19.2.9	19.2.9
19.1 antes de 19.1.9	19.1.9
19.0 antes de 19.0.10	19.0.10
Del 7 al 18 de noviembre, antes del 18 de noviembre de 2013.	18.11.13

Cuatro de estas versiones son anteriores a las que la compañía suele mantener con actualizaciones de seguridad. Su política habitual contempla la versión vigente y las dos versiones mensuales previas, que, a la fecha indicada, corresponden a las ramas 19.5, 19.4 y 19.3.

La empresa informó que incorporó la corrección a las versiones 18.11.13, 19.0.10, 19.1.9 y 19.2.9, además de sus lanzamientos habituales. Este tipo de actualización retroactiva se reserva para problemas considerados especialmente graves.

El motivo por el que la vulnerabilidad afecta a versiones tan antiguas se encuentra en el componente que presenta el fallo. El compilador de expresiones regulares utiliza el motor integrado de Ruby, denominado Onigmo, que GitLab incluye en sus propios paquetes y modifica durante la creación de sus compilaciones. Debido a que el defecto reside en ese motor, está presente en todas las versiones de GitLab que lo incorporan, es decir, desde la versión 7.0.

Asimismo, GitLab publicó dos reglas de detección para ayudar a los administradores de instalaciones autogestionadas a identificar posibles intentos de explotación. Estas reglas reciben los nombres de “Onigmo native worker crash” y “Org mode render error burst”. Ambas forman parte de TLDR, el marco de trabajo de código abierto de la compañía, que utiliza el formato Sigma para definir reglas de detección basadas en los registros de la propia aplicación de GitLab.

GitLab todavía no ha detallado qué condiciones previas necesita cumplir un atacante para acceder al compilador. En consecuencia, los administradores no pueden descartar el riesgo únicamente a partir de la configuración de sus sistemas. La instalación de la corrección constituye la única medida de protección plenamente confirmada, ya que el aviso de seguridad de la empresa no contempla ninguna solución temporal.

Esta es la cuarta vulnerabilidad relacionada con la ejecución de código en el motor de expresiones regulares de GitLab que el mismo investigador, identificado con el alias joaxcar, ha reportado en el transcurso de un mes. También es la primera de estas vulnerabilidades que afecta a versiones anteriores a la 19.2.

El 12 de octubre, GitLab corrigió la vulnerabilidad CVE-2026-97229, otro fallo por desbordamiento en el compilador de expresiones regulares, con una puntuación CVSS de 10.0 y explotable sin autenticación. La solución se incorporó a las versiones 19.2.8, 19.3.5 y 19.4.2. Posteriormente, el 23 de septiembre, la empresa solucionó otras dos vulnerabilidades: CVE-2026-93577 y CVE-2026-89078. Ambas recibieron una puntuación de 9.9, aunque para explotarlas era necesario contar con una sesión iniciada. Los tres fallos anteriores afectaban a versiones a partir de la rama 19.2, mientras que la vulnerabilidad más reciente también alcanza versiones anteriores.

La publicación del 21 de octubre incluye correcciones para un total de 11 problemas de seguridad. Uno se clasifica como crítico, mientras que los diez restantes se distribuyen entre los niveles alto, medio y bajo.

Otros dos fallos están relacionados con los mecanismos de autenticación. La vulnerabilidad CVE-2026-15723, con una clasificación alta de 8.2, podría permitir que un usuario autenticado tomara el control de otra cuenta. Sin embargo, para que esto ocurra, un administrador debe haber habilitado simultáneamente SAML y la vinculación automática de cuentas mediante LDAP.

Por otra parte, la vulnerabilidad CVE-2026-112212 afecta a los mecanismos de OAuth y a los puntos de acceso de OpenID Connect de GitLab. Este problema de envenenamiento de

caché, clasificado como alto con una puntuación de 7.5, podría permitir que un atacante redirigiera determinados procesos de inicio de sesión hacia un servidor bajo su control, siempre que la infraestructura utilice una caché compartida.

La actualización también implica ciertos aspectos operativos que deben planificarse. Las versiones 19.4.3 y 19.3.6 incorporan modificaciones en la base de datos que se ejecutan durante el proceso de actualización. En los servidores de un solo nodo, estas operaciones provocan una interrupción del servicio mientras finalizan. En cambio, GitLab señala que las infraestructuras con varios nodos pueden instalar el parche sin interrumpir el servicio, siempre que sigan el procedimiento establecido para realizar actualizaciones con tiempo de inactividad cero.