La plataforma DevOps GitLab emitió esta semana parches para abordar una vulnerabilidad crítica en su software, que podría conducir a la ejecución de código arbitrario en los sistemas afectados.

Rastreada como CVE-2022-2884, la vulnerabilidad tiene una calificación de 9.9 en el sistema de calificación de vulnerabilidad CVSS, e impacta a todas las versiones de GitLab Community Edidion (CE) y Enterprise Edition (EE) a partir de 11.3.4 antes de 15.1.5, 15.2 antes de 15.2.3 y 15.3 antes de 15.3.1.

En esencia, la debilidad de la seguridad es un caso de ejecución de código remoto autenticado que se puede activar a través de la API de importación de GitHub. GitLab brindó el crédito a yvvdwf por descubrir y reportar la vulnerabilidad.

Aunque el problema se resolvió en las versiones 15.3.1, 15.2.3, 15.1.5, los usuarios también tienen la opción de protegerse contra la falla al deshabilitar temporalmente la opción de importación de GitHub:

- Hacer clic en Menú > Administrador
- Hacer clic en Configuración > General
- Expandir la pestaña Visibilidad y controles de acceso
- En Importar fuentes, deshabiliar la opción GitHub
- Hacer clic en Guardar cambios

No existe evidencia de que el problema esté siendo explotado en ataques en estado salvaje. Aún así, se recomienda a los usuarios que ejecutan una instalación afectada que actualicen a la última versión lo más pronto posible.