Tecnológico de Costa Rica

Escuela de Ingeniería en Computación

Seguridad del software - IC8700

Vulnerabilidad en el Software

Estudiante:
Axel Alexander Chaves Reyes - 2021099588

Profesor:
Herson Esquivel Vargas

Semestre I

2024

CVE-2024-0402

Cuando los desarrolladores e ingenieros de software trabajan con proyectos programados, deben contar con un respaldo del trabajo que están haciendo. Es así como surgen distintas herramientas de control de versiones para el código de dichos proyectos, tales como Git, Monotone, Mercurial, entre otras. La herramienta de control de versiones más popular es Git y sus ramas GitHub y GitLab, lo cual genera una diversidad de usuarios y necesidades.

GitLab es la rama de Git más empresarial que no solo ofrece control de versiones, sino distintos servicios a los cuales diversos roles como DevOps sacan provecho. Asimismo, la demanda y tipo de uso de este servicio requiere que sus criterios de calidad y seguridad satisfagan las necesidades de sus usuarios, no obstante, ningún software está exento de ser vulnerado.

El 25 de Junio de 2024, Greg Myers, ingeniero de seguridad de aplicaciones de GitLab publicó un artículo donde explica que lanzaron un parche de seguridad crítico para GitLab, debido a que encontraron un problema en GitLab en sus versiones para la comunidad y para empresas, el cual afecta a las versiones 16.0 hasta 16.6.6 y 16.7 hasta 16.7.4.

Asimismo, el fallo identificado con el código CVE-2024-0402 radica en un fallo que permite a un usuario autenticado escribir archivos en ubicaciones arbitrarias en el servidor de GitLab mientras se crea un espacio de trabajo. Además, a dicho ataque se le conoce como *path traversal*.

Path traversal se refiere a una técnica de hacking que permite que un individuo acceda a ficheros de una aplicación sin contar con suficientes permisos, es decir, sin contar con una debida autorización (KeepCoding, 2023).

Según GitLab, esta vulnerabilidad fue encontrada por Joern Schneeweisz, quien, para fortuna de la empresa, es parte del equipo de seguridad e investigación. En adición, se catalogó este problema como crítico, debido a que este fallo de seguridad puede provocar que un atacante lo explote y obtenga o inyecte información sensible en el sistema.

De acuerdo a la calificación dada a este fallo por el Sistema Común de Puntuación de Vulnerabilidades (CVSS, por sus siglas en inglés), este problema tiene una nota de 9.9 sobre 10, debido a que la complejidad del ataque es baja y el impacto en confidencialidad, integridad y disponibilidad es muy alto. Por fortuna, la empresa no ha recibido perjuicio alguno dado que lograron identificar este problema a tiempo.

En síntesis, el equipo encargado de la seguridad de aplicaciones de GitLab logró controlar una vulnerabilidad que daba acceso no autorizado a usuarios para que hicieran modificaciones en el sistema, demostrando así la importancia de un personal capacitado para identificar debilidades en el software.

Referencias

KeepCoding. (2023, November 1). *¿Qué es path traversal?*. KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-path-traversal/

Myers, G. (n.d.). *Gitlab critical security release: 16.8.1, 16.7.4, 16.6.6, 16.5.8*. GitLab. https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/#arbitrary-file-write-while-creating-workspace