Atlassian implementó correcciones para una vulnerabilidad de seguridad crítica en Bitbucket Server and Data Center, que podría conducir a la ejecución de código malicioso en instalaciones vulnerables.

Rastreada como CVE-2022-36804 (puntaje CVSS: 9.9), la vulnerabilidad se caracterizó como una falla de inyección de comandos en múltiples puntos finales, que podría explotarse a través de solicitudes HTTP especialmente diseñadas.

> *«Un atacante con acceso a un repositorio público de Bitbucket o con permisos de lectura a uno privado puede ejecutar código arbitrario enviando una solicitud HTTP maliciosa»,* dijo Atlassian.

La vulnerabilidad, descubierta e informada por el investigador de seguridad @TheGrandPew, afecta a todas las versiones de Bitbucket Server and Data Center lanzadas después de la 6.10.17, incluyendo la 7.0.0 y posteriores.

- Servidor Bitbucket y centro de datos 7.6
- Bitbucket Server y centro de datos 7.17
- Bitbucket Server y centro de datos 7.21
- Bitbucket Server y Centro de datos 8.0
- Servidor Bitbucket y centro de datos 8.1
- Bitbucket Server y Datacenter 8.2
- Servidor Bitbucket y centro de datos 8.3

Como solución temporal en escenarios en los que los parches no se pueden aplicar inmediatamente, Atlassian recomienda desactivar los repositorios públicos usando *«feature.public.access=false»* para evitar que los usuarios no autorizados aprovechen la falla.

> *«Esto no puede considerarse una mitigación completa, ya que un atacante con una*

> *cuenta de usuario aún podría tener éxito»,* dijo la empresa.