Se han dado a conocer dos nuevas vulnerabilidades de seguridad en el software JetBrains TeamCity On-Premises que podrían ser aprovechadas por un actor de amenazas para tomar el control de los sistemas afectados.

Estas fallas, identificadas como CVE-2024-27198 (puntuación CVSS: 9.8) y CVE-2024-27199 (puntuación CVSS: 7.3), han sido abordadas en la versión 2023.11.4. Afectan a todas las versiones de TeamCity On-Premises hasta la 2023.11.3.

> Según JetBrains, *«estas vulnerabilidades podrían permitir a un atacante no autenticado con acceso HTTP(S) a un servidor TeamCity evadir las verificaciones de autenticación y obtener control administrativo sobre dicho servidor TeamCity.»* Este aviso fue publicado el lunes.

Cabe destacar que las instancias de TeamCity Cloud ya han sido actualizadas para corregir estas dos vulnerabilidades. La empresa de ciberseguridad Rapid7, que descubrió y reportó los problemas el 20 de febrero de 2024, explicó que CVE-2024-27198 implica una elusión de autenticación que permite la completa compromisión de un servidor susceptible por parte de un atacante remoto no autenticado.

> *«La compromisión de un servidor TeamCity otorga al atacante un control total sobre todos los proyectos, construcciones, agentes y artefactos de TeamCity, convirtiéndolo en un vector adecuado para llevar a cabo un ataque en la cadena de suministro»*, señaló la empresa.

En cuanto a CVE-2024-27199, también una falla de elusión de autenticación, se origina en un problema de recorrido de ruta que permite a un atacante no autenticado reemplazar el certificado HTTPS en un servidor TeamCity vulnerable con un certificado de su elección a través del punto final *«/app/https/settings/uploadCertificate»,* incluso modificar el número de puerto en el que el servicio HTTPS escucha.

Esta vulnerabilidad podría ser explotada por un actor de amenazas para llevar a cabo un ataque de denegación de servicio contra el servidor TeamCity, ya sea cambiando el número de puerto HTTPS o cargando un certificado que no pase la validación del lado del cliente. Alternativamente, el certificado cargado podría utilizarse en escenarios de ataque en el que el atacante se interpone entre las comunicaciones si es confiado por los clientes.

Rapid7 destacó que esta elusión de autenticación permite llegar a un número limitado de puntos finales autenticados sin autenticación. *«Un atacante no autenticado podría aprovechar esta vulnerabilidad para modificar un conjunto limitado de configuraciones del sistema en el servidor y, además, revelar una cantidad limitada de información sensible»,* afirmó la empresa.

Este desarrollo ocurre casi un mes después de que JetBrains lanzara correcciones para abordar otra falla (CVE-2024-23917, puntuación CVSS: 9.8) que también podría permitir a un atacante no autenticado obtener control administrativo de los servidores TeamCity.

Dado que las vulnerabilidades de seguridad en JetBrains TeamCity fueron objeto de explotación activa el año pasado por actores de amenazas de Corea del Norte y Rusia, es imperativo que los usuarios tomen medidas inmediatas para actualizar sus servidores.