Atlassian y el Consorcio de Sistemas de Internet (ISC) han divulgado múltiples defectos de seguridad que afectan a sus productos y que podrían ser aprovechados para lograr una negación de servicio (DoS) y ejecución de código remoto.

El proveedor australiano de servicios de software informó que las cuatro fallas de alta gravedad fueron corregidas en nuevas versiones lanzadas el mes pasado. Estas incluyen:

- CVE-2022-25647 (puntuación CVSS: 7.5): Una vulnerabilidad de deserialización en el paquete Google Gson que impacta en la Administración de Parches en Jira Service Management Data Center y Server.
- CVE-2023-22512 (puntuación CVSS: 7.5): Una falla de DoS en Confluence Data Center y Server.
- CVE-2023-22513 (puntuación CVSS: 8.5): Una vulnerabilidad de ejecución remota de código (RCE) en Bitbucket Data Center y Server.
- CVE-2023-28709 (puntuación CVSS: 7.5): Una falla de DoS en el servidor Apache Tomcat que afecta a Bamboo Data Center y Server.

Las fallas han sido abordadas en las siguientes versiones:

Jira Service Management Server y Data Center (versiones 4.20.25, 5.4.9, 5.9.2, 5.10.1, 5.11.0 o posteriores).
Confluence Server y Data Center (versiones 7.19.13, 7.19.14, 8.5.1, 8.6.0 o posteriores).
Bitbucket Server y Data Center (versiones 8.9.5, 8.10.5, 8.11.4, 8.12.2, 8.13.1, 8.14.0 o posteriores).
Bamboo Server y Data Center (versiones 9.2.4, 9.3.1 o posteriores).

Dos Defectos de Alta Gravedad en BIND Corregidos:

En un desarrollo relacionado, ISC ha emitido soluciones para dos errores de alta gravedad que afectan al conjunto de software del Sistema de Nombres de Dominio de Internet de Berkeley (BIND) 9 que podrían conducir a una condición de DoS:

- CVE-2023-3341 (puntuación CVSS: 7.5): Una falla de agotamiento de la pila en el código del canal de control podría provocar que «named» se cierre de manera inesperada (corregido en versiones 9.16.44, 9.18.19, 9.19.17, 9.16.44-S1 y 9.18.19-S1).
- CVE-2023-4236 (puntuación CVSS: 7.5): El servicio «named» podría finalizar inesperadamente bajo una carga elevada de consultas DNS sobre TLS (corregido en versiones 9.18.19 y 9.18.19-S1).

Las últimas actualizaciones llegan tres meses después de que ISC lanzara soluciones para otros tres defectos en el software (CVE-2023-2828, CVE-2023-2829 y CVE-2023-2911, puntuaciones CVSS: 7.5) que podrían resultar en una condición de DoS.