

BOLETÍN DE ALERTA

Boletín Nro.: 2024-03

Fecha de publicación: 17/01/2024

Tema: Vulnerabilidad de severidad crítica permite ejecución de código remoto en productos Atlassian Confluence

Productos afectados:

- Confluence Data Center, versión 7.9.0 (CVE-2023-22526)
- Confluence Data Center y Server, version 2.10 (CVE-2024-21672) y versiones 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x y 8.5.0 a 8.5.3 (CVE-2023-22527)

Descripción:

Se ha reportado una vulnerabilidad de severidad crítica, identificada como CVE-2023-22527 con puntuación CVSS de 10.0, de inyección de código arbitrario en las plantillas de proyectos del sistema afectado, que podría permitir a un atacante no autenticado, lograr ejecución remota de código (RCE) en una versión afectada.

Además, han identificado otras 28 vulnerabilidades de gravedad alta, destacando dos de ellas (CVE-2023-22526 y CVE-2024-21672) que podrían permitir la ejecución remota de código en los sistemas afectados de Confluence. Para más detalles de estas, se puede verificar en el siguiente enlace:

<https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html>

Impacto:

Estas vulnerabilidades permitirían a un actor malicioso no autenticado, ejecutar código de forma remota en el sistema afectado, permitiendo tomar control total del mismo.

Recomendación:

El fabricante no ha publicado soluciones alternativas, por lo cual se recomienda de forma urgente aplicar parches y actualizaciones publicados por Atlassian en su sitio web oficial.

Información adicional:

- <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-atlassian-0>
- <https://www.bleepingcomputer.com/news/security/atlassian-warns-of-critical-rce-flaw-in-older-confluence-versions/>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-22527>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-22526/change-record?changeRecordedOn=01/16/2024T00:15:07.933-0500>
- <https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html>

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Offic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

