Alerta de seguridad cibernética	9VSA24-00958-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2024
Última revisión	18 de enero de 2024

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de vulnerabilidades que afectan a varios productos de Atlassian, incluyendo una crítica en Confluence Data Center y Data Center and Server.

Vulnerabilidades

- CVE-2022-42252
- CVE-2023-22527
- CVE-2020-25649
- CVE-2022-44729
- CVE-2021-40690
- CVE-2023-46589
- CVE-2023-3635
- CVE-2023-22526
- CVE-2024-21672
- CVE-2024-21673
- CVE-2024-21674
- CVE-2023-43642
- CVE-2023-6481
- CVE-2023-6378
- CVE-2023-46589
- CVE-2023-34455
- CVE-2023-34454
- CVE-2023-34453
- CVE-2023-36478
- CVE-2023-5072
- CVE-2023-36478
- CVE-2023-39410

CVE-2020-26217
CVE-2017-7957
CVE-2022-4244
CVE-2018-10054
CVE-2023-5072
CVE-2023-46589
CVE-2022-40152

Impacto

Vulnerabilidad de riesgo crítico:

CVE-2023-22527: Error de inyección de templates que podría ser explotado para conseguir ejecución remota de código sin necesidad de autenticación. CVSS: 10.

Mitigación

CVE-2023-22527: La empresa indica que la mayor parte de las versiones aún con soporte no son afectadas por esta vulnerabilidad porque ha sido mitigada en actualizaciones regulares. Quienes tengan versiones desactualizadas deben actualizar de inmediato al menos a la versión 8.5.4 (LTS) para Confluence Data Center and Server, y 8.6.0 y 8.7.1 de Confluence Data Center.

Parchar según producto:
Bitbucket Data Center: 7.21.21, 8.9.9, 8.13.5, 8.14.4, 8.15.3, 8.16.2, 8.17.0 o más reciente
Bitbucket Server: 7.21.21, 8.9.9, 8.13.5, 8.14.4
Bamboo Data Center and Server: 9.2.9, 9.3.6, 9.4.2 o más reciente.
Jira Data Center and Server:9.4.13, 9.7.0 o más reciente
Jira Service Management Data Center and Server:4.20.30, 5.4.15, 5.12.2 o más reciente
Crowd Data Center and Server:5.2.2 o más reciente
Confluence Data Center:7.19.18, 8.5.5, 8.7.2 o más reciente
Confluence Server:7.19.18, 8.5.5

Productos afectados

CVE-2023-22527: Confluence Data Center y Confluence Server, versiones desactualizadas (8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x y 8.5.0-8.5.3)

Bitbucket Data Center
Bitbucket Server
Bamboo Data Center and Server
Jira Data Center and Server
Jira Service Management Data Center and Server
Crowd Data Center and Server
Confluence Data Center
Confluence Server

Enlaces
https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html
https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.18 15:39:56 -03'00'