Atlassian ha lanzado soluciones para abordar una vulnerabilidad crítica de día cero que actualmente está siendo explotada de manera activa y que afecta a las instancias de Confluence Data Center y Server de acceso público.

Esta vulnerabilidad, identificada como CVE-2023-22515, es susceptible de ser explotada de forma remota y permite a atacantes externos crear cuentas no autorizadas de administrador en Confluence y obtener acceso a los servidores de Confluence.

Es importante destacar que esta vulnerabilidad no afecta a las versiones de Confluence anteriores a la 8.0.0, y los sitios de Confluence accesibles a través de un dominio atlassian.net no son vulnerables a este problema.

El proveedor de servicios de software empresarial indicó que tuvo conocimiento de este problema gracias a *«un reducido número de clientes».* La vulnerabilidad ha sido resuelta en las siguientes versiones de Confluence Data Center y Server:

- 8.3.3 o versiones posteriores
- 8.4.3 o versiones posteriores
- 8.5.2 (versión de soporte a largo plazo) o versiones posteriores

No obstante, la compañía no proporcionó detalles adicionales acerca de la naturaleza y la extensión de la explotación, ni sobre la causa raíz de la vulnerabilidad.

Para aquellos clientes que no puedan aplicar las actualizaciones, se recomienda restringir el acceso de red externo a las instancias afectadas.

> *«Atlassian también sugiere que se pueden mitigar los vectores de ataque conocidos para esta vulnerabilidad bloqueando el acceso a los puntos de conexión /setup/* en las instancias de Confluence. Esto se puede lograr a nivel de red o mediante la implementación de los siguientes cambios en los archivos de configuración de Confluence»,* mencionó la compañía.

Asimismo, Atlassian ha proporcionado indicadores de compromiso (IoC) para determinar si una instancia local podría haber sido comprometida:

- La presencia inesperada de miembros en el grupo confluence-administrator.
- La creación inesperada de cuentas de usuario.
- Solicitudes a /setup/*.action registradas en los registros de acceso de red.
- La existencia de /setup/setupadministrator.action en un mensaje de excepción en atlassian-confluence-security.log en el directorio principal de Confluence.

Atlassian aconseja que si se determina que una instancia de Confluence Server/DC ha sido comprometida, se proceda a apagarla y desconectarla de la red/Internet de inmediato. Además, se sugiere apagar cualquier otro sistema que comparta una base de usuarios o tenga combinaciones de nombre de usuario y contraseña comunes con el sistema comprometido.

> *«Cabe mencionar que es inusual, aunque no sin precedentes, que una vulnerabilidad de escalada de privilegios se califique con una gravedad crítica. Por lo general, este tipo de fallo está más relacionado con eludir la autenticación o ejecutar código de manera remota que con un problema de escalada de privilegios por sí mismo»*, según Caitlin Condon de Rapid7.

Dado que en el pasado se han observado numerosos casos de actores de amenazas explotando vulnerabilidades en las instancias de Atlassian Confluence, se recomienda a los clientes que actualicen a una versión corregida de manera inmediata o que implementen las medidas de mitigación apropiadas.