Atlassian lanzó el viernes correcciones para abordar una vulnerabilidad de seguridad crítica que afecta a sus productos Confluence Server y Data Center, que han sido explotados activamente por hackers para lograr la ejecución remota de código.

Rastreada como CVE-2022-26134, una vulnerabilidad similar a CVE-2021-26084, otra falla que la compañía de software australiana corrigió en agosto de 2021.

Ambos errores se relacionan con un caso de inyección de Object-Graph Navigation Language (OGNL) que podría explotarse para lograr la ejecución de código arbitrario en una instancia de Confluence Server o Data Center.

La deficiencia recién descubierta afecta a todas las versiones compatibles de Confluence Server y Data Center, y todas las versiones posteriores a la 1.3.0 también se ven afectadas. Se resolvió en las siguientes versiones:

- 7.4.17
- 7.13.7
- 7.14.3
- 7.15.2
- 7.16.4
- 7.17.4
- 7.18.1

Según las estadísticas de la plataforma de descubrimiento de activos de Internet Censys, existen alrededor de 9325 servicios en 8347 hosts distintos que ejecutan una versión vulnerable de Atlassian Confluence, con la mayoría de las instancias ubicadas en Estados Unidos, China, Alemania, Rusia y Francia.

La evidencia de la explotación activa de la vulnerabilidad, probablemente por parte de atacantes chinos, salió a la luz luego de que la compañía de seguridad cibernética Volexity descubriera la falla durante el fin de semana del Día de los Caídos en Estados Unidos, durante una investigación de respuesta a incidentes.

> *«Las industrias/verticales objetivo están bastante extendidas. Esta es una batalla campaña en la que la explotación parece coordinada»*, dijo Steven Adair, fundador y presidente de Volexity.

> *«Está claro que múltiples grupos de amenazas y actores individuales tienen el exploit y lo han estado usando de distintas maneras. Algunos son bastante descuidados y otros son un poco más sigilosos».*

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), además de agregar la vulnerabilidad de día cero a su Catálogo de Vulnerabilidades Explotadas Conocidas, también ha instado a las agencias federales a bloquear inmediatamente todo el tráfico de Internet hacia y desde los productos afectados y aplicar los parches o eliminar las instancias antes del 6 de junio de 2022.