Investigadores de ciberseguridad han hallado un backdoor sigiloso denominado Effluence, desplegado tras el aprovechamiento exitoso de una reciente vulnerabilidad de seguridad en Atlassian Confluence Data Center y Server.

> *«Este malware actúa como un backdoor persistente y no se elimina aplicando parches a Confluence»,* señaló Aon's Stroz Friedberg Incident Response Services en un análisis publicado esta semana.

> *«Este backdoor proporciona la capacidad de realizar un movimiento lateral hacia otros recursos de la red, además de la exfiltración de datos desde Confluence. Lo crucial es que los atacantes pueden acceder a este backdoor de manera remota sin autenticarse en Confluence».*

La cadena de ataque documentada por la entidad de ciberseguridad implicó la explotación de CVE-2023-22515 (puntuación CVSS: 10.0), un fallo crítico en Atlassian que podría ser utilizado para crear cuentas de administrador no autorizadas en Confluence y acceder a los servidores de Confluence.

Desde entonces, Atlassian ha revelado una segunda vulnerabilidad conocida como CVE-2023-22518 (puntuación CVSS: 10.0) que un atacante también puede aprovechar para establecer una cuenta de administrador falsa, lo que resulta en una pérdida total de confidencialidad, integridad y disponibilidad.

Lo que resalta en este último ataque es que el adversario obtuvo acceso inicial a través de CVE-2023-22515 e incrustó un nuevo shell web que proporciona acceso remoto persistente a cada página web en el servidor, incluida la página de inicio de sesión no autenticada, sin necesidad de una cuenta de usuario válida.

Este shell web, compuesto por un cargador y una carga útil, es pasivo, permitiendo que las

solicitudes pasen desapercibidas hasta que se proporcione una solicitud que coincida con un parámetro específico, momento en el cual desencadena su comportamiento malicioso mediante la ejecución de una serie de acciones.

Esto incluye la creación de una nueva cuenta de administrador, la eliminación de registros para encubrir el rastro forense, la ejecución de comandos arbitrarios en el servidor subyacente, la enumeración, lectura y eliminación de archivos, y la recopilación de información extensa sobre el entorno de Atlassian.

Según Aon, el componente del cargador actúa como un plugin normal de Confluence y es responsable de descifrar y lanzar la carga útil.

> *«Varias de las funciones del shell web dependen de las APIs específicas de Confluence»,* afirmó el investigador de seguridad Zachary Reichert.

> *«Sin embargo, el plugin y el mecanismo de carga parecen depender solo de las APIs comunes de Atlassian y son potencialmente aplicables a JIRA, Bitbucket u otros productos de Atlassian donde un atacante pueda instalar el plugin».*