Los perpetradores de amenazas están aprovechando la falta de actualizaciones en los servidores de Atlassian para implantar una variante de Cerber (también conocido como C3RB3R) ransomware diseñada para Linux.

Estos ataques se valen de la vulnerabilidad de seguridad CVE-2023-22518 (con una puntuación CVSS de 9.1), que afecta gravemente al Atlassian Confluence Data Center y Server, permitiendo a un atacante no autenticado reiniciar Confluence y crear una cuenta de administrador.

Con este acceso, un actor malicioso podría tomar el control de los sistemas afectados, lo que resultaría en una pérdida total de confidencialidad, integridad y disponibilidad.

De acuerdo con la empresa de seguridad en la nube Cado, se ha observado que grupos delictivos motivados financieramente están abusando de la cuenta de administrador recién creada para instalar el plugin de shell web Effluence, lo que permite la ejecución de comandos arbitrarios en el servidor.

Nate Bill, ingeniero de inteligencia de amenazas en Cado, mencionó en un informe que: *«El atacante utiliza este shell web para descargar y ejecutar el cargador primario de Cerber».*

> *«En una configuración por defecto, la aplicación Confluence se ejecuta como el usuario 'confluence', un usuario con bajos privilegios. Por lo tanto, los datos que el ransomware puede cifrar están limitados a los archivos propiedad del usuario 'confluence'».*

Es importante destacar que la explotación de CVE-2023-22518 para desplegar Cerber ransomware ya fue señalada anteriormente por Rapid7 en noviembre de 2023.

Escrito en C++, el cargador primario actúa como un intermediario para malware adicional basado en C++, recuperándolos de un servidor de control de comando (C2) y luego eliminando su propia presencia del host infectado.

Incluye un archivo llamado «*agttydck.bat*«, que se ejecuta para descargar el cifrador («agttydcb.bat») que luego es ejecutado por el cargador primario.

Se sospecha que agttydck actúa como un verificador de permisos para el malware, evaluando su capacidad para escribir en un archivo /tmp/ck.log. Sin embargo, el propósito exacto de esta verificación no está claro.

Por otro lado, el cifrador recorre el directorio raíz y cifra todo el contenido con una extensión .L0CK3D, además de dejar una nota de rescate en cada directorio. A pesar de lo que se afirma en la nota, no hay exfiltración de datos.

El aspecto más interesante de estos ataques es el uso de cargas útiles escritas en C++, lo cual es poco común debido al cambio hacia lenguajes de programación multiplataforma como Golang y Rust.

> Bill comentó: *«Cerber es una carga útil de ransomware relativamente sofisticada, aunque ya tiene sus años». «Si bien la explotación de la vulnerabilidad de Confluence le permite comprometer una gran cantidad de sistemas valiosos, a menudo los datos que puede cifrar están limitados a los de Confluence y, en sistemas bien configurados, estos estarán respaldados».*
>
> *«Esto limita enormemente la eficacia del ransomware para extorsionar dinero a las víctimas, ya que hay menos incentivo para pagar»,* añadió el investigador.

Este desarrollo ocurre en medio del surgimiento de nuevas familias de ransomware como Evil Ant, HelloFire, L00KUPRU (una variante de ransomware Xorist), Muliaka (basada en el código filtrado del ransomware Conti), Napoli (una variante de ransomware Chaos), Red CryptoApp, Risen, y SEXi (basada en el código filtrado del ransomware Babuk), que han sido vistas atacando servidores Windows y VMware ESXi.

Los perpetradores de ransomware también están aprovechando el código fuente filtrado del ransomware LockBit para crear sus propias variantes personalizadas como Lambda (también conocida como Synapse), Mordor y Zgut, según informes de F.A.C.C.T. y Kaspersky.

El análisis de Kaspersky de los archivos de construcción filtrados de LockBit 3.0 ha revelado la *«alarmante simplicidad»* con la que los atacantes pueden crear ransomware personalizado y aumentar sus capacidades con funciones más potentes.

Kaspersky dijo que descubrió una versión adaptada con la capacidad de propagarse por la red a través de PsExec aprovechando credenciales de administrador robadas, así como realizar actividades maliciosas como terminar Microsoft Defender Antivirus y borrar los registros de eventos de Windows para cifrar datos y cubrir sus huellas.

> *«Esto subraya la necesidad de medidas de seguridad sólidas capaces de mitigar eficazmente este tipo de amenaza, así como la adopción de una cultura de ciberseguridad entre los empleados»,* dijo la empresa.