Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUE DE RANSOMWARE CERBER EXPLOTA VULNERABILIDAD CRÍTICA EN SERVIDORES ATLASSIAN

17 / 04 / 2024

CONTENIDO

INTRODUCCIÓN

Se aborda un caso de intrusión cibernética que comenzó con un reinicio de Confluence y la creación de una cuenta de administrador, así obteniendo acceso total al sistema comprometido. El encargado, Cerber Ransomware, también conocido como C3RBER, es altamente utilizado por una variedad de grupos delictivos que han sido motivados financieramente. Estos instalan un plugin de web shell llamado ”Effluence” el cual les permite ejecutar comandos arbitrarios ene el servidor comprometido.

ATAQUE DE RANSOMWARE CERBER EXPLOTA VULNERABILIDAD CRÍTICA EN SERVIDORES ATLASSIAN

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_04_17_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	17/04/2024
Es día cero (0 day):	No

RESUMEN

El mundo de la ciberseguridad enfrenta un nuevo desafío con la explotación de una grave vulnerabilidad en servidores de Atlassian, que ha permitido la propagación de una variante de ransomware Cerber en sistemas Linux.

Detalles del Ataque

Los ciberdelincuentes están aprovechando una vulnerabilidad crítica, identificada como CVE-2023-22518, que afecta a los servidores de Atlassian Confluence Data Center y Server. Esta vulnerabilidad permite a un atacante no autenticado reiniciar Confluence y crear una cuenta de administrador, obteniendo así acceso total al sistema comprometido.

Descripción del Ransomware

El ransomware Cerber, también conocido como C3RB3R, es utilizado por grupos delictivos con motivaciones financieras. Tras obtener acceso mediante la vulnerabilidad de Atlassian, los atacantes instalan un plugin de web shell llamado Effluence, que les permite ejecutar comandos arbitrarios en el servidor comprometido.

Impacto del Ataque

Aunque la aplicación Confluence se ejecuta con privilegios limitados, el ransomware es capaz de cifrar archivos pertenecientes al usuario "confluence". Sin embargo, en sistemas bien configurados, esta limitación reduce la cantidad de datos susceptibles de cifrado.

Método de Propagación

El ransomware utiliza cargas útiles escritas en C++ para su ejecución. A través de un proceso complejo, se descarga y ejecuta el cifrador que encripta archivos en el directorio raíz con una extensión ".L0CK3D", dejando una nota de rescate en cada directorio afectado.

A pesar de la sofisticación del ataque, es fundamental resaltar la importancia de contar con medidas de seguridad robustas. Además, la concientización sobre ciberseguridad entre los empleados es esencial para prevenir este tipo de amenazas.

Evolución del Ransomware

Este ataque se suma a la creciente amenaza de nuevas familias de ransomware, como Evil Ant, HelloFire y otras, que han sido observadas atacando servidores Windows y VMware ESXi.

Llamado a la Acción

Ante la complejidad de estas amenazas, es crucial implementar medidas de seguridad proactivas y promover una cultura de ciberseguridad en todas las organizaciones.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240417_1_CerberRansomware

NOTICIA COMPLETA

https://devel.group/blog/ataque-de-ransomware-cerber-explota-vulnerabilidad-critica-en-servidores-atlassian/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente