Nro. Alerta:	AL-2024-021	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		V 1.1
Fecha:	17-oct-2024	VULNERABILIDAD CVE-2024-40711 EN VEEAM	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Vulnerabilidad

Nivel de riesgo: Alto

II. ALERTA

El equipo de investigación de amenazas de Florian Hauser de Code White Gmbh reportó una vulnerabilidad de deserialización insegura en Veeam Backup & Replication.

Identificada como (CVE-2024-40711), la explotación exitosa de la vulnerabilidad podría llevar a la ejecución remota de código (RCE). La RCE podría permitir a los atacantes ejecutar código en un dispositivo remoto sin necesidad de acceso físico.

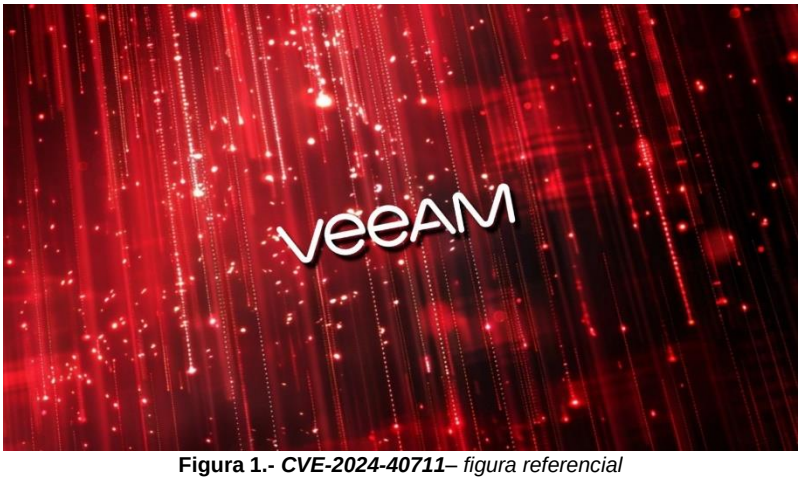

Figura 1.- ***CVE-2024-40711****– figura referencial*

III. INTRODUCCIÓN.

Los piratas informáticos están explotando una vulnerabilidad crítica en el software Veeam Backup & Replication, identificada como CVE-2024-40711, para implementar ransomware.

Según se informa, estos grupos están explotando CVE-2024-40711 como un exploit de segunda etapa para crear nuevas cuentas de administrador local para facilitar objetivos adicionales en redes comprometidas.

Como falla de ejecución remota de código (RCE) no autenticada, la vulnerabilidad tiene un puntaje CVSS de 9.8 y amenaza entornos que ejecutan versiones 12.1.2.172 y anteriores.

Durante el último mes, la falla RCE CVE-2024-40711 fue rápidamente detectada y explotada en ataques de ransomware Akira y Fog, junto con credenciales previamente comprometidas para agregar una cuenta local a los grupos locales de Administradores y Usuarios de Escritorio Remoto.

En un caso, los atacantes instalaron con éxito el ransomware Fog en un servidor Hyper-V desprotegido, mientras que en otro ataque intentaron implementar el ransomware Akira.

Los atacantes inicialmente obtuvieron acceso a los objetivos utilizando puertas de enlace VPN comprometidas sin autenticación multifactor habilitada, algunas de las cuales ejecutaban versiones de software no compatibles.

En el incidente del ransomware Fog, los atacantes no solo implementaron el ransomware, sino que también utilizaron la utilidad rclone para extraer datos confidenciales del sistema comprometido.

Estos incidentes resaltan la importancia de parchear vulnerabilidades conocidas, actualizar o reemplazar VPN fuera de soporte y usar autenticación multifactor para controlar el acceso remoto.

Al momento, Veeam publicó dos recomendaciones para abordar diferentes componentes de la vulnerabilidad. El primer parche, la versión 12.1.2.172, hizo que las credenciales de bajo nivel siguieran siendo necesarias para que los

actores de amenazas explotaran la vulnerabilidad. El segundo parche, la versión 12.2.0.334, resuelve completamente la falla. Es posible que la vulnerabilidad fuera más grave de lo que Veeam inicialmente dejó ver y que el primer parche no mitigara por completo la amenaza de RCE, dejando los sistemas expuestos y provocando un segundo intento de parcheo.

IV. VECTOR DE ATAQUE:

CVE-2024-40711, Vulnerabilidad clasificada como crítica que permite la ejecución remota de código no autenticado (RCE). La vulnerabilidad de Veeam se explota al activar Veeam.Backup.MountService.exe en el URI /trigger del puerto 8000, lo que generó net.exe y creó una cuenta local denominada “point”. Esta cuenta se agregó a los grupos de usuarios locales Administradores y Escritorio remoto , lo que otorgó a los atacantes acceso privilegiado al sistema para luego implementar ramsomware.

V. RECOMENDACIONES:

- Asegurarse de que todas las puertas de enlace de acceso remoto a su organización estén protegidas, actualizadas, auditadas regularmente y, lo más importante, que tengan implementada la autenticación multifactor (MFA), preferiblemente de la variedad resistente al phishing.

- Aplicar las actualizaciones remitidas por los fabricantes.

VI. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.

- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VII. REFERENCIAS:

https://www.bleepingcomputer.com/news/security/akira-and-fog-ransomware-now-exploiting-critical-veeam-rce-flaw/

https://securityaffairs.com/169679/cyber-crime/ransomware-groups-exploit-veeam-backup-replication-bug.html

https://securityaffairs.com/169679/cyber-crime/ransomware-groups-exploit-veeam-backup-replication-bug.html

https://cybersecuritynews.com/hackers-exploiting-veeam-rce-vulnerability/

https://www.darkreading.com/application-security/poc-exploit-for-rce-flaw-but-patches-from-veeam

https://www.veeam.com/kb4649

https://www.infosecurity-magazine.com/news/nhs-england-warns-cve-active/