Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CYBERARK ABORDA VULNERABILIDADES CRÍTICAS CON PARCHES DE SEGURIDAD

22 / 01 / 2025

CONTENIDO

INTRODUCCIÓN

Se aborda un caso de intrusión cibernética que comenzó con un acceso no autorizado a un host RDP expuesto, utilizando credenciales legítimas de la cuenta de Administrador predeterminada. Lo destacado de este ataque radica en la ausencia de intentos de fuerza bruta, sugiriendo la posibilidad de acceso previo recurrente o la intervención de un intermediario de acceso. Una vez dentro, los perpetradores desplegaron diversas herramientas, incluyendo scripts por lotes, ejecutables y SoftPerfect Netscan, para realizar escaneos de red, identificar comparticiones y explorar documentos. La intrusión avanzó con movimientos laterales, deshabilitación de Windows Defender y exfiltración de datos hacia Mega.io mediante Rclone. La sorpresa llegó cuando, tras una desconexión, los atacantes se reconectaron desde una dirección IP diferente, indicando un conocimiento profundo de la red.

CYBERARK ABORDA VULNERABILIDADES CRÍTICAS CON PARCHES DE SEGURIDAD

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

ID de alerta:	DSOC-CERT_2025_01_22_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	22/01/2025
Es día cero (0 day):	No

RESUMEN

El 22 de enero de 2025, CyberArk emitió cuatro boletines de seguridad críticos que abordan vulnerabilidades significativas en sus productos. A continuación, se detallan las vulnerabilidades y sus resoluciones:

CA25-01: Vulnerabilidad en el despliegue de HTML5 Gateway (RPM)

- **Severidad:** Alta (CVSS: 8.7)
- **CVE:** CVE-2024-38286
- **Impacto:** Potencial Denegación de Servicio (DoS) debido a una vulnerabilidad en Tomcat.
- **Productos afectados:**
  - Self-Hosted HTML5 Gateway (RPM deployment) versiones 14.0 y 14.2.
- **Resolución:**
  - Actualizar a las versiones parcheadas:
    - 14.0.1
    - 14.2.1

CA25-02: Elevación de privilegios en Vault y PVWA Self-Hosted

- **Severidad:** Alta (CVSS: 7.1)
- **Impacto:** Posibilidad de obtener autorización para mostrar cuentas.
- **Productos afectados:**
  - Vault y PVWA Self-Hosted en versiones anteriores a 14.4.1.
- **Resolución:**
  - Actualizar a las versiones parcheadas:
    - Vault 14.4.1 y PVWA 14.4.1
    - Vault 14.2.2 y PVWA 14.2.2.
    - Vault 12.6.13 y PVWA 12.6.14.

CA25-03: Vulnerabilidad de elevación de privilegios en PVWA Self-Hosted

- **Severidad:** Alta (CVSS: 8.3)
- **Impacto:** Posibilidad de obtener funcionalidad de desbloqueo de cuentas.
- **Productos afectados:**
  - PVWA Self-Hosted en versiones 14.0, 14.2 y 14.4.
- **Resolución:**
  - Actualizar a las versiones parcheadas:
    - PVWA 14.4.1
    - PVWA 14.2.2
    - PVWA 14.0.4

CA25-04: Acceso no autorizado a cuentas mediante mensajes especialmente diseñados

- **Severidad:** Alta (CVSS: 7.1)
- **Impacto:** Potencial para que usuarios no autorizados accedan a cuentas.
- **Productos afectados:**
  - Vault Self-Hosted en versiones anteriores a 14.4.

- **Resolución:**
    - Actualizar a las versiones parcheadas:
        - Vault 14.2.2
        - Vault 14.0.3
        - Vault 12.6.13

Es fundamental implementar las actualizaciones proporcionadas por CyberArk para proteger los entornos corporativos y minimizar los riesgos asociados con estas vulnerabilidades. ***Los clientes que requieran asistencia para planificar y ejecutar la mitigación de estas vulnerabilidades pueden comunicarse con nuestro equipo especializado a través del correo electrónico tac@devel.group.*** Nuestro equipo está preparado para brindar soporte y guía profesional en este proceso.

NOTICIA COMPLETA

https://devel.group/blog/cyberark-aborda-vulnerabilidades-criticas-con-parches-de-seguridad/

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://devel.group/