Boletín informativo
Vulnerabilidad en RecoverPoint for Virtual Machines de DELL

CSIRTSALUD-AV-20260218-30 **TLP: AMBER**

Alerta ID:	030
Fecha del reporte:	18/02/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en RecoverPoint for Virtual Machines de DELL
Herramienta de detección	N/A
Activo involucrado:	Dell RecoverPoint for Virtual Machines (RP4VM)
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Crítico

Resumen ejecutivo

Informar a las entidades del Ecosistema Digital sobre una vulnerabilidad de "día cero" (zero-day) activamente explotada en dispositivos Dell RecoverPoint. El objetivo es facilitar la identificación de sistemas vulnerables, detectar posibles intrusiones previas y guiar el proceso de remediación inmediata para evitar el compromiso de los activos de recuperación ante desastres.

Descripción:

La vulnerabilidad **CVE-2026-22769** se debe al uso de **credenciales codificadas (hardcoded credentials)** en el archivo de configuración de Apache Tomcat (tomcat-users.xml) dentro del appliance de Dell.

Dell ha notificado a los usuarios afectados sobre las versiones de Dell RecoverPoint para máquinas virtuales anteriores a la 6.0.3.1 HF1 contienen una vulnerabilidad de credenciales codificadas. Esto se considera crítico, ya que un atacante remoto no autenticado que posea

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

conocimiento de estas credenciales puede acceder a la interfaz del **Tomcat Manager** y, desde allí, desplegar archivos maliciosos con privilegios elevados. Debido a que RecoverPoint gestiona copias de seguridad y replicación, un compromiso aquí permite al atacante manipular la capacidad de recuperación de toda la organización.

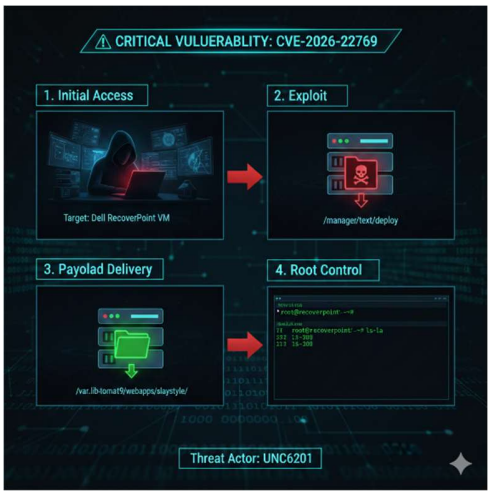
A diferencia de un ataque convencional, este ha sido utilizado de forma silenciosa por el clúster **UNC6201**. Los atacantes aprovechan estas credenciales para autenticarse remotamente y desplegar archivos WAR maliciosos a través del endpoint /manager/text/deploy, obteniendo privilegios de **root** de forma inmediata y persistente.

Modo de explotación y cadena de infección

La explotación de la **CVE-2026-22769** no es un evento aislado, sino una secuencia sofisticada diseñada para el espionaje a largo plazo. Se divide en las siguientes fases críticas:

1. **Acceso Inicial y Despliegue de persistencia volátil**

El ataque comienza con una solicitud no autenticada al servicio **Apache Tomcat Manager** integrado en el appliance. Al utilizar las credenciales administrativas embebidas en el archivo tomcat-users.xml, el atacante abusa del endpoint de gestión /manager/text/deploy.



Cargan un archivo .war malicioso que despliega el web shell **SLAYSTYLE**, proporcionando una interfaz de comandos con privilegios de **root** directamente sobre el sistema operativo Linux del appliance.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

2. Evasión de Defensas mediante Compilación Nativa (GRIMBOLT)

Una vez establecido el acceso, el actor de amenaza transiciona a backdoors más robustos. La evolución de **BRICKSTORM** hacia **GRIMBOLT** (detectada en sept. 2025) marca un hito en sofisticación:

GRIMBOLT está escrito en C# pero utiliza compilación **Native AOT (Ahead-of-Time)**. Esto transforma el código en binarios nativos del sistema, eliminando el rastro de metadatos de .NET que las herramientas de EDR y escáneres de malware suelen identificar.

El binario es empacado adicionalmente con **UPX** para complicar el análisis estático y la ingeniería inversa.

3. Persistencia en el Arranque del Sistema

Para asegurar su permanencia tras reinicios del sistema, el atacante no se limita a tareas programadas comunes.

Modifican el script legítimo del sistema /usr/bin/convert_hosts.sh. Este script es llamado por procesos de inicialización de Dell, permitiendo que el malware se ejecute de forma transparente mediante rc.local cada vez que el equipo se enciende, mimetizándose con los servicios de recuperación de desastres.

4. Pivoteo mediante "Ghost NICs" (Redes Fantasma)

Esta es la fase más innovadora del ataque. Para moverse lateralmente hacia el entorno de **VMware vCenter** o infraestructuras **SaaS** sin alertar a los sistemas de monitoreo de red (NMS):

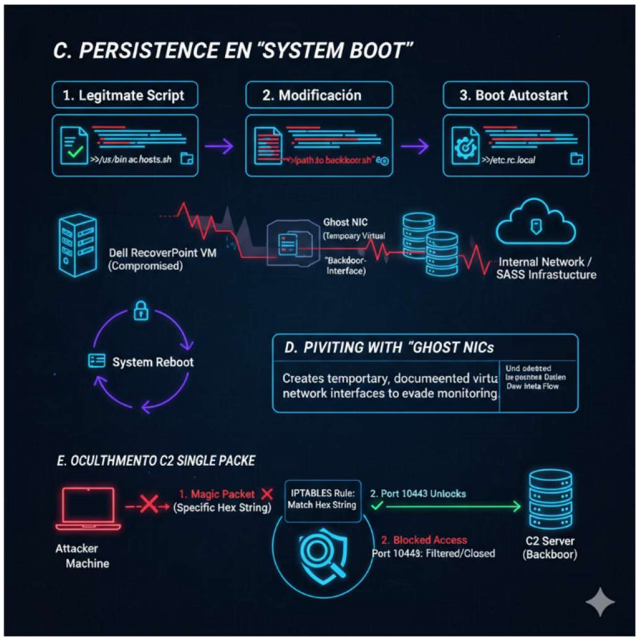
CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

El atacante crea interfaces de red virtuales temporales directamente en el kernel de los hosts ESXi comprometidos. Estas "Ghost NICs" permiten un túnel de comunicación privado para extraer datos o saltar a otros servidores. Una vez cumplido el objetivo, las interfaces son eliminadas, borrando la ruta lógica del ataque.

5. Ocultamiento de C2 (Single Packet Authorization)

El tráfico de Comando y Control (C2) se oculta mediante una técnica de "golpeo de puertos" avanzada:

- El atacante envía un **paquete mágico** (una cadena hexadecimal específica) al puerto 443.
- Un script de iptables monitorea el tráfico; al detectar la cadena, añade la IP del atacante a una lista de permitidos.
- Solo entonces, las conexiones al puerto **10443** son aceptadas, mientras que, para cualquier otro usuario o escáner de red, el puerto parece cerrado o redirigido, haciendo que el backdoor sea virtualmente invisible.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

La vulnerabilidad de credenciales codificadas suele alinearse con las siguientes tácticas y técnicas (MITRE ATT&CK)

Táctica	Técnica	Descripción
Acceso Inicial	T1190 – Exploit Public-Facing Application	La vulnerabilidad puede explotarse remotamente a través de una interfaz web expuesta.
Persistencia	T1098 – Account Manipulation	Tras obtener acceso administrativo/root, el atacante puede crear o modificar cuentas para mantener acceso persistente.
Escalada de Privilegios	T1078 – Valid Accounts	Las credenciales embebidas otorgan privilegios elevados directamente, permitiendo control completo del sistema.
Evasión de Defensas	T1036 – Masquerading	El uso de credenciales legítimas dificulta la detección, ya que el acceso parece autorizado.
Impacto	T1496 – Resource Hijacking	Posible despliegue de ransomware tras comprometer el sistema.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Indicadores de compromiso

Los siguientes hashes y nombres han sido asociados a actividad maliciosa vinculada a CVE-2026-22769:

Backdoors y malware desplegados

- **GRIMBOLT** backdoor (implant persistente, compilado con AOT):
  - ✓ **SHA-256:** 24a11a26a2586f4fba7bfe89df2e21a0809ad85069e442da98c37c4add369a0c
  - ✓ **SHA-256:** dfb37247d12351ef9708cb6631ce2d7017897503657c6b882a711c0da8a9a591

Web shell y WAR maliciosos

- **SLAYSTYLE web shell** (implant vía Apache Tomcat):
  - ✓ **SHA-256:** 92fb4ad6dee9362d0596fda7bbcfe1ba353f812ea801d1870e37bfc6376e624a

Familia BRICKSTORM

- **SHA-256:** aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878
- **SHA-256:** 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df
- **Otros hashes asociados:**
  - ✓ 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759
  - ✓ 90b760ed1d0cb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035
  - ✓ 45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Indicadores de Red:

- **C2 IP:** 149.248.11.71
- **C2 Endpoint:** wss://149.248.11.71/rest/apisession

Recomendaciones

- **Inspección de Interfaces:** Verificar en VMware vCenter la existencia de adaptadores de red no documentados o temporales en los hosts ESXi.

- **Análisis de Scripts de Inicio:** Revisar si el archivo /usr/bin/convert_hosts.sh ha sido modificado para invocar binarios sospechosos al arranque.

- **Monitoreo de iptables:** Buscar reglas inusuales que redirijan tráfico del puerto 443 al 10443 basándose en contenido de paquetes (inspección profunda).

Solución y Remediación

1. **Actualización Crítica:** Es obligatorio subir a la versión **6.0.3.1 HF1** o superior. Esta versión elimina las credenciales hardcoded.
2. **Ruta de Migración:**
    - Si posee versión **5.3 SP4 P1**: Migrar a 6.0 SP3 y luego aplicar el parche 6.0.3.1 HF1.
    - Si posee versiones **5.3 SP4 o anteriores**: Aplicar urgentemente el script de remediación de Dell **DSA-2026-079**.
3. **Aislamiento de Red:** Los appliances de RecoverPoint **no deben estar expuestos a Internet**. Deben residir en una zona de gestión (OOB) con acceso restringido mediante firewalls y segmentación estricta.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fuentes:

- https://www.cve.org/CVERecord?id=CVE-2026-22769
- https://cwe.mitre.org/data/definitions/798.html
- https://cwe.mitre.org/data/images/CWE-798-Diagram.png
- https://nvd.nist.gov/vuln/detail/CVE-2026-22769
- https://thehackernews.com/2026/02/dell-recoverpoint-for-vms-zero-day-cve.html
- https://cybersecuritynews.com/dell-0-day-vulnerability/
- https://www.bleepingcomputer.com/news/security/chinese-hackers-exploiting-dell-zero-day-flaw-since-mid-2024/

Este evento presenta un riesgo critico si no se cuentas con las medidas de seguridad bien establecidas iniciando principalmente con actualizaciones de los servidores, la defensa de un servidor ya no se limita a bloquear intrusos externos, sino que requiere una auditoría interna exhaustiva de cada módulo y cada llamada al sistema.

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570