Boletín informativo vulnerabilidades “ReVault”

CSIRTSALUD-AL-20250808-12 **TLP: AMBER**

Incidente ID:	0012
Fecha del reporte:	08/08/2025
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades “ReVault” asociadas a portátiles Dell
Herramienta de detección	Análisis de fuentes oficiales Dell
Activo involucrado:	Modelos de Portátiles Dell
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre las vulnerabilidades críticas en los portátiles Dell, conocidas como 'ReVault', que afectan a más de 100 modelos, permitiendo la ejecución remota de código, el robo de datos biométricos y el acceso persistente al firmware, incluso tras una reinstalación del sistema operativo

Boletín informativo vulnerabilidades “ReVault”

CSIRTSALUD-AL-20250808-12 **TLP: AMBER**

Descripción:

Una amplia gama de vulnerabilidades afecta a millones de equipos portátiles Dell utilizados por agencias gubernamentales, profesionales de ciberseguridad y empresas de todo el mundo.

Las vulnerabilidades, denominadas colectivamente “ReVault”, apuntan **al chip de seguridad Broadcom BCM5820X** integrado en el **firmware ControlVault3 de Dell**, lo que crea oportunidades para que los atacantes roben contraseñas, datos biométricos y mantengan acceso persistente a los sistemas comprometidos.

Actualmente las vulnerabilidades afectan a más de 100 modelos diferentes de computadoras portátiles Dell, principalmente de las series **Latitude** y **Precision** enfocadas en negocios que se implementan ampliamente en entornos sensibles.

Vector de impacto:

Ejecución remota de código en firmware, Robo de datos biométricos almacenados, Acceso persistente tras reinstalación o cambio de disco, Compromiso profundo del sistema a nivel firmware, Riesgo de control total del dispositivo.

Los investigadores de Cisco Talos identificaron cinco vulnerabilidades críticas que afectan a los componentes de seguridad **Dell ControlVault3** (versiones anteriores a la 5.15.10.14) y **Dell ControlVault3+** (versiones anteriores a la 6.2.26.36), presentes en múltiples modelos de portátiles Dell. Estas vulnerabilidades podrían permitir desde la fuga de información hasta la

ejecución remota de código, comprometiendo la integridad y confidencialidad del dispositivo a nivel de firmware.

Vulnerabilidades identificadas:

- **CVE-2025-24311:** Lectura fuera de límites que permite fuga de información sensible.
- **CVE-2025-25050:** Escritura fuera de límites que posibilita ejecución remota de código.
- **CVE-2025-25215:** Vulnerabilidad de memoria libre arbitraria, que puede causar corrupción de memoria.
- **CVE-2025-24922:** Desbordamiento de búfer en pila que permite ejecución arbitraria de código.
- **CVE-2025-24919:** Fallo de deserialización insegura en APIs Windows de ControlVault, abriendo puertas a ataques remotos.

Modelos afectados:

A continuación, se presentan algunos ejemplos de los modelos afectos para las vulnerabilidades "ReVault"

Dell Pro Series:

- Pro 13 Plus (PB13250), Pro 14 Plus (PB14250), Pro 16 Plus (PB16250), Pro Max 14 (MC14250), Pro Max 16 (MC16250), Pro Rugged 13 (RA13250), Pro Rugged 14 (RB14250)

Dell Latitude Series:

- Latitude 5300 y 5300 2-in-1, 5310 y 5310 2-in-1, 5320, 5330, 5340, 5350

- 5400, 5401, 5410, 5411, 5420, 5421, 5430 (incluyendo modelo Rugged), 5431, 5440, 5450
- 5500, 5501, 5510, 5511, 5520, 5521, 5530, 5531, 5540, 5550
- Rugged Extreme 7030, 7200 2-in-1, 7210 2-in-1, 7220 Rugged Extreme, 7230 Rugged Extreme
- 7300, 7310, 7320 y 7320 Detachable, 7330 (varios), 7340, 7350 y 7350 Detachable
- 7400, 7400 2-in-1, 7410, 9410, 9510

Recomendaciones de mitigación:

Pasos de Remediación Urgente

1- **Verificar si el equipo está afectado**

Consultar la lista oficial de modelos afectados en el siguiente enlace

- https://www.dell.com/support/kbdoc/en-us/000276106/dsa-2025-053?utm_source

2- **Verificar la versión del firmware instalada**

Acceder al sitio de soporte de Dell e ingresar el número de serie (Service Tag) del equipo para verificar la versión del firmware **ControlVault3 / ControlVault3 Plus** instalada

3- **Descargar la actualización**

Desde el mismo sitio de soporte, descargar la versión **corregida** del firmware disponible para el modelo afectado

4- **Instalar la actualización**

- Ejecutar el archivo descargado y seguir las instrucciones del asistente de instalación
- Reiniciar el equipo una vez completada la instalación

5- Confirmar la actualización

Verificar nuevamente en el sitio de Dell que la versión instalada sea la recomendada en el aviso DSA-2025-053.

Recomendaciones adicionales:

- Aplicar esta actualización en todos los equipos afectados.
- Priorizar la actualización en equipos utilizados en áreas sensibles o por personal con acceso privilegiado.
- Mantener el BIOS y otros controladores del sistema actualizados.

Fuentes:

- https://cybersecuritynews.com/dell-laptops-vulnerability/#google_vignette
- https://www.dell.com/support/kbdoc/en-us/000276106/dsa-2025-053?utm_source
- https://androidtr.es/vulnerabilidades-revault-dell/

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) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.