BOLETÍN DE ALERTA

Boletín Nro.: 2021-10

Fecha de publicación: 13/05/2021

Tema: Vulnerabilidades críticas en el control de acceso en el controlador Dell dbutil_2_3.sys.

Versiones que se ven afectadas:

- cpe: 2.3: a: dell: dbutil_2_3.sys: -: *: *: *: *: *: *: *

Descripción

Cientos de millones de computadoras Dell en todo el mundo se ven afectadas por una vulnerabilidad de 12 años, rastreada como **CVE-2021-21551** de severidad **alta** con puntuación **8.8**, que afecta al controlador Dell DBUtil. La falla afecta a la versión 2.3 del controlador de BIOS de Dell, es uno de una serie de problemas de escalamiento de privilegios descubiertos por investigadores de SentinelLabs.

Estas múltiples vulnerabilidades de alta gravedad en el software de Dell podrían permitir a los atacantes escalar los privilegios de un usuario que no es administrador a los privilegios del modo kernel. A lo largo de los años, Dell ha lanzado utilidades de actualización de BIOS que contienen el controlador vulnerable para cientos de millones de computadoras (incluidas computadoras de escritorio, portátiles y tabletas) en todo el mundo.

A continuación se expone la lista de vulnerabilidades de gravedad alta reportadas por los expertos:

- **CVE-2021-21551:** Elevación local de privilegios n° 1: corrupción de memoria
- **CVE-2021-21551:** Elevación local de privilegios n° 2: corrupción de memoria
- **CVE-2021-21551:** Elevación local de privilegios n° 3: falta de validación de entrada
- **CVE-2021-21551:** Elevación local de privilegios n° 4: falta de validación de entrada
- **CVE-2021-21551:** Denegación de servicio: problema de lógica de código

Impacto:

El controlador **Dell dbutil_2_3.sys** contiene una vulnerabilidad de control de acceso insuficiente que puede provocar una escalada de privilegios, denegación de servicio o divulgación de información. Se requiere acceso de usuario autenticado local.

Solución y mitigación

- Instale un paquete corregido que contenga el BIOS, el firmware Thunderbolt, el firmware TPM o el firmware de la base.
- Actualizar Dell Command Update, Dell Update o Alienware Update.
- Instalar la última versión de Dell System Inventory Agent o Dell Platform Tags.

Los usuarios afectados deben completar los 2 pasos siguientes:

- Elimine inmediatamente el controlador dbutil_2_3.sys vulnerable del sistema afectado a continuación: descargue y ejecute una utilidad para eliminar el controlador del sistema, elimine manualmente el controlador del sistema, o a partir del 10 de mayo de 2021, utilice una de las soluciones de notificación de Dell para ejecutar la utilidad.
    - El archivo del controlador mencionado se puede ubicar en los siguientes directorios.
        - C: \Users\<nombre de usuario>\AppData\Local\Temp
        - C: \Windows\Temp
- A continuación, obtenga y ejecute los últimos paquetes de utilidades de actualización de firmware, Dell Command Update, Dell Update, Alienware Update, Dell System Inventory Agent o Dell Platform Tags según corresponda.

Referencias

- https://www.dell.com/support/kbdoc/es-py/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability
- https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2021-21551
- https://www.lansweeper.com/vulnerability/dell-bios-driver-software-receives-patch-to-fix-critical-security-issues-cve-2021-21551/
- https://securityaffairs.co/wordpress/117514/security/cve-2021-21551-dell-flaws.html