BOLETÍN DE ALERTA

Boletín Número: 2021-05 **Fecha de Publicación:** 28/06/2021

Tema: Múltiples vulnerabilidades en BIOSConnect y HTTPS Boot de Dell Client BIOS

Importancia: Alta

Resumen:

Se han reportado 4 vulnerabilidades: 3 de severidad alta y 1 media, que afectan a las funcionalidades BIOSConnect y HTTPS Boot incluídas en Dell Client BIOS, que podrían permitir a un atacante ejecutar código arbitrario en el nivel BIOS/UEFI del dispositivo afectado.:

Las vulnerabilidades fueron catalogadas con los siguientes identificadores CVE-2021-21573, CVE-2021-21574, CVE-2021-21571 y CVE-2021-21572.

Recursos Afectados:

El problema afecta a 129 modelos diferentes de portátiles, tabletas y ordenadores de sobremesa Dell, y al menos a 30 millones de dispositivos individuales. El listado completo de productos afectados puede encontrarse en la sección "Información adicional" del aviso de Dell.

Descripción:

La función Dell BIOSConnect contiene una vulnerabilidad de desbordamiento de búfer. Un atacante autenticado, con privilegios de administrador y con acceso local al sistema, podría explotar esta vulnerabilidad para ejecutar código arbitrario y saltarse las restricciones de UEFI. Comprometer la BIOS de un dispositivo daría al atacante la posibilidad de controlar el proceso de carga del sistema operativo del host y desactivar las protecciones para no ser detectado, lo que permitiría establecer una persistencia continua mientras controla el dispositivo afectado con alto nivel de privilegios. Se han asignado los identificadores CVE-2021-21572, CVE-2021-21573 y CVE-2021-21574, para estas vulnerabilidades de severidad alta.

La pila https de Dell UEFI BIOS, potenciada por las funciones Dell BIOSConnect y Dell HTTPS Boot, contiene una vulnerabilidad de validación de certificados inadecuada. Un atacante remoto, no autenticado, podría explotar esta vulnerabilidad utilizando un ataque de MitM (man-in-the-middle) que podría conducir a una condición de

denegación de servicio (DoS) y a la manipulación de la carga útil (payload tampering). Se ha asignado el identificador CVE-2021-21571 para esta vulnerabilidad de severidad media.

Riesgos:

- Ejecución de código arbitrario
- Saltarse las restricciones de UEFI
- control del proceso de carga del sistema operativo
- Ataque MitM (man-in-the-middle)
- Divulgación de información

Solución:

- Actualizar la BIOS/UEFI del sistema en todos los sistemas afectados.
- No utilizar BIOSConnect para realizar esta actualización del firmware.
- En su lugar, se aconseja ejecutar el archivo de actualización de la BIOS desde el sistema operativo después de contrastar manualmente los hashes con los publicados por Dell.
- Las vulnerabilidades CVE-2021-21573 y CVE-2021-21574 fueron solucionadas en el lado del servidor el 28 de mayo de 2021 y no requieren ninguna acción adicional del cliente.

Referencias:

https://www.dell.com/support/kbdoc/es-es/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-biosconnect-feature-and-https-boot-feature
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-bioconnect-y-https-boot-dell-client