El fabricante de computadoras Dell, publicó una actualización para corregir múltiples vulnerabilidades críticas de escalada de privilegios que no fueron detectadas desde 2009, lo que potencialmente permite a los atacantes obtener privilegios en modo kernel y causar una condición de denegación de servicio.

Los problemas, informados a Dell por investigadores de SentinelOne el 1 de diciembre de 2020, residen en un controlador de actualización de firmware llamado *«dbutil_2_3.sys»*, que viene preinstalado en sus dispositivos. Al parecer, cientos de millones de computadoras de escritorio, portátiles y tabletas fabricadas por la compañía son vulnerables.

> *«El controlador Dell dbutil_2_3.sys contiene una vulnerabilidad de control de acceso insuficiente que puede conducir a una escalada de privilegios, denegación de servicio o divulgación de información. Se requiere acceso de usuario autenticado local»,* dijo Dell en un aviso.

A las cinco vulnerabilidades se les asignó el identificador CVE-2021-21551 con una puntuación CVSS de 8.8. Se desglosan de la siguiente forma:

- CVE-2021-21551: Elevación local de privilegios no. 1: corrupción de memoria
- CVE-2021-21551: Elevación local de privilegios no. 2: corrupción de memoria
- CVE-2021-21551: Elevación local de privilegios no. 3: falta de validación de entrada
- CVE-2021-21551: Elevación local de privilegios no. 4: falta de validación de entrada
- CVE-2021-21551: Denegación de servicio: problema de lógica de código

> *«Las vulnerabilidades de alta gravedad podrían permitir a cualquier usuario en la computadora, incluso sin privilegios, escalar sus privilegios y ejecutar código en modo kernel. Entre los abusos obvios de tales vulnerabilidades se encuentran que podrían usarse para eludir productos de seguridad»,* dijo Kasif Dekel, investigador de SentinelOne.

Debido a que se trata de vulnerabilidades de escalada de privilegios locales, es poco probable que se exploten de forma remota a través de Internet. Para llevar a cabo un ataque, un adversario deberá haber obtenido acceso a una cuenta que no sea de administrador en un sistema vulnerable, luego de lo cual se puede abusar de la vulnerabilidad del controlador para obtener una elevación local de privilegios. Armado con este acceso, el atacante puede aprovechar otras técnicas para ejecutar código arbitrario y moverse lateralmente a través de la red de una organización.

Aunque no se ha encontrado evidencia de abuso en la naturaleza, SentinelOne dijo que planea lanzar el código de prueba de concepto (PoC) el 1 de junio de 2021, dando a los clientes de Dell tiempo suficiente para corregir la vulnerabilidad.

La divulgación de SentinelOne cuenta como la tercera que informa el mismo problema a Dell en los últimos dos años. Según el arquitecto jefe de Crowdstrike, Alex Ionescu, primero por la compañía de seguridad con sede en Sunnyvale en 2019 y nuevamente por IOActive. Dell también le dio crédito a Scott Noone de OSR Open Systems Resources por reportar la vulnerabilidad.