
La utilidad SupportAssist de Dell que viene preinstalada en millones de computadoras portátiles y PC de Dell, contiene una vulnerabilidad de seguridad que podría permitir que software malicioso o los usuarios sin acceso registrados, escalen sus privilegios a nivel de administrador y accedan a información confidencial.

Descubierta por investigadores de seguridad en SafeBreach Labs, la vulnerabilidad, identificada como CVE-2019-12280, es un problema de escalada de privilegios y afecta la aplicación SupportAssist de Dell para PC empresariales (versión 2.0) y PC domésticas (versión 3.2.1 y todas las versiones anteriores).

Dell SupportAssist, anteriormente conocido como Dell System Detect, verifica el estado del hardware y software de su sistema, alertando a los clientes para que tomen las medidas adecuadas para resolverlos. Para hacerlo, se ejecuta en su computadora con permisos de nivel SYSTEM.

Con estos privilegios de alto nivel, la utilidad interactúa con el sitio web de soporte de Dell y detecta automáticamente la etiqueta de servicio o el código de servicio rápido de su producto Dell, escanea los controladores de dispositivo existentes e instala actualizaciones de controladores faltantes o disponibles, junto con la realización de pruebas de diagnóstico de hardware.

Sin embargo, los investigadores de SafeBreach Labs descubrieron que el software carga de forma insegura archivos .dll desde carpetas controladas por el usuario cuando se ejecuta, dejando un lugar para el malware y los usuarios maliciosos que inician sesión para corromper las DLL existentes o reemplazarlas por otras maliciosas.

Por lo tanto, cuando SupportAssist carga esas DLL contaminadas, el código malicioso se inyecta en el programa y se ejecuta dentro del contexto de un

administrador, lo que permite al atacante obtener el control completo de un sistema de destino.

"Según el sitio web de Dell, SupportAssist está preinstalado en la mayoría de los dispositivos Dell que ejecutan Windows. Esto significa que mientras el software no tenga parches, la vulnerabilidad afecta a millones de usuarios de computadoras Dell", dicen los investigadores.

¿Qué es preocupante? Los investigadores creen que Dell no es la única compañía cuyas PC se ven afectadas por este problema de seguridad en particular.

Dado que Dell SupportAssist está escrito y mantenido por la empresa de diagnóstico y atención al cliente con sede en Nevada PC-Doctor , otros fabricantes de PC que agrupan las mismas herramientas de diagnóstico y solución de problemas en sus propias computadoras con diferentes nombres también pueden ser vulnerables.

"Después de que SafeBreach Labs enviara los detalles a Dell, descubrimos que esta vulnerabilidad afecta a los OEM adicionales que usan una versión renombrada de los componentes de software PC-Doctor Toolbox para Windows", dicen los investigadores.

Además, según el sitio web de PC-Doctor , los fabricantes de PC han "preinstalado más de 100 millones de copias de PC-Doctor para Windows en sistemas informáticos de todo el mundo", lo que significa que la falla también afecta a otros OEM que confían en PC-Doctor para la resolución de problemas especializados herramientas.

Dado que el software SupportAssist de Dell utiliza un controlador firmado por PC-Doctor para acceder a la memoria y al hardware de bajo nivel, los investigadores demostraron esta vulnerabilidad al leer el contenido de una dirección de memoria física arbitraria como prueba de concepto.

SafeBreach Labs informó la vulnerabilidad a Dell el 29 de abril de 2019, y la compañía luego informó el problema a PC Doctor y lanzó las correcciones proporcionadas por PC-Doctor el 28 de mayo para las versiones afectadas de SupportAssist.

Se recomienda a los usuarios de Dell Business y Home PC que actualicen su software a Dell SupportAssist for Business PCs versión 2.0.1 y Dell SupportAssist for Home PCs versión 3.2.2 respectivamente.

Fuente: https://thehackernews.com/2019/06/dells-supportassist-hacking.html