Bill Demirkapi, investigador de seguridad independiente de solo 17 años, descubrió una vulnerabilidad crítica de ejecución remota de código en la utilidad Dell SupportAssist que viene preinstalada en la mayoría de computadoras Dell.

Dell SupportAssis, antes conocido como Dell System Detect, verifica el estado del hardware y el software de la computadora.

La utilidad ha sido diseñada para interactuar con el sitio web de asistencia de Dell y detectar automáticamente la etiqueta de servicio o el código de servicio rápido del producto Dell, escanear los controladores de dispositivos existentes e instalar actualizaciones de controladores faltantes o disponibles, así como realizar pruebas de diagnóstico de hardware.

Dell SupportAssist ejecuta en segundo plano un servidor web localmente en el sistema de usuario, ya sea en los puertos 8884, 8883, 8886 o 8885, y acepta varios comandos como parámetros de URL para realizar tareas predefinidas en la computadora, como recopilar información detallada del sistema o descargar un software desde un servidor remoto e instalarlo en el sistema.

Aunque el servicio web local ha sido protegido utilizando el encabezado de respuesta *«Access-Control-Allow-Origin»* y tiene algunas validaciones que lo restringen para aceptar comandos solo desde el sitio web «dell.com» o sus subdominios, Demirkapi explicó las formas de evitar las protecciones en una publicación.

En el video siguiente Demirkapi demostró cómo los piratas informáticos remotos podrían haber descargado e instalado fácilmente el malware de un servidor remoto en las computadoras Dell afectadas para tomar control total sobre ellos.

> *«Un atacante no autenticado, que comparte la capa de acceso a la red con el sistema vulnerable, puede comprometer al sistema vulnerable engañando a un usuario víctima para que descargue y ejecute archivos ejecutables arbitrarios por medio del cliente SupportAssist desde los sitios hospedados por el atacante»,* dijo la

> compañía en un aviso.

La vulnerabilidad de ejecución remota de código, identificada como CVE-2019-3719, afecta a las versiones de Dell SupportAssist Client anteriores a la versión 3.2.0.90.

Antes de hacer públicos los detalles de la vulnerabilidad, el investigador informó de manera responsable sus hallazgos al equipo de seguridad de Dell, que ahora lanzó una versión actualizada del software afectado para solucionar el problema.

Ademas de este problema, Dell también solucionó una vulnerabilidad de validación de origen incorrecta (CVE-2019-3718) en el software SupportAssist que podría haber permitido a un atacante remoto no autenticado intentar ataques CSRF en los sistemas de los usuarios.

Se recomienda a los usuarios de Dell que instalen SupportAssist 3.2.0.90 actualizado, o simplemente desinstalar la aplicación si no es necesaria, antes de que los hackers intenten explotar las debilidades para controlar sus computadoras.