Investigadores de seguridad cibernética revelaron este 21 de diciembre dos vulnerabilidades críticas de seguridad en los clientes Dell Wyse Thin, que podrían haber permitido a los hackers ejecutar remotamente código malicioso y acceder a archivos arbitrarios en los dispositivos afectados.

Las vulnerabilidades, descubiertas por el proveedor de ciberseguridad de atención médica, CyberMDX, y reportadas a Dell en junio de 2020, afectan a todos los dispositivos que ejecutan ThinOS con versiones 8.6 y anteriores.

Dell abordó las dos vulnerabilidades en una actualización publicada esta semana. Las fallas tienen una puntuación CVSS de 10 sobre 10.

Rastreadas como CVE-2020-29491 y CVE-2020-29492, las vulnerabilidades de seguridad en los clientes Thin de Wyse se deben al hecho de que las sesiones FTP utilizadas para extraer actualizaciones de firmware y configuraciones de un servidor local están desprotegidas sin autenticación, lo que hace posible que un atacante en la misma red lea y altere las configuraciones.

El primer defecto, CVE-2020-29491, permite al usuario acceder al servidor y leer configuraciones (archivos .ini) pertenecientes a otros clientes.

La segunda vulnerabilidad (CVE-2020-29492), permite que al no tener credenciales FTP, cualquier persona en la red pueda acceder al servidor FTP y alterar directamente los archivos .ini que contienen la configuración de otros dispositivos Thin.

Cabe señalar que la configuración puede incluir datos confidenciales, como posibles contraseñas e información de la cuenta que podría usarse para comprometer el dispositivo.

Debido a la facilidad de explotación de las vulnerabilidades, se recomienda que los parches se apliquen lo antes posible.

CyberMDX también recomienda actualizar los clientes compatibles a ThinOS 9, que elimina la

función de administración de archivos INI. En caso de que una actualización no sea factible, se recomienda deshabilitar el uso de FTP para recuperar los archivos vulnerables y, en su lugar, confiar en un servidor HTTPS o Wyse Management Suite.

> *«Leer o alterar esos parámetros abre la puerta a una variedad de escenarios de ataque. Configurar y habilitar VNC para un control remoto completo, filtrar credenciales de escritorio remoto y manipular los resultados de DNS son algunos de los escenarios a tener en cuenta»,* dijeron los investigadores de CyberMDX.