Investigadores de seguridad cibernética revelaron este domingo múltiples vulnerabilidades críticas en el software de monitoreo remoto de estudiantes, Netop Vision Pro, que un atacante podría abusar para ejecutar código arbitrario y apoderarse de computadoras con sistema Windows.

> *«Estos hallazgos permiten la elevación de privilegios y la ejecución remota de código en última instancia, que podría ser utilizado por un atacante malintencionado dentro de la misma red para obtener el control total sobre los ordenadores de los alumnos»,* dijo el equipo de investigación de amenazas de McAfee Labs.

Las vulnerabilidades, rastreadas como CVE-2021-27192, CVE-2021-27193, CVE-2021-27194 y CVE-2021-27195, se informaron a Netop el 11 de diciembre de 2020. Después de eso, la empresa con sede en Dinamarca solucionó los problemas en una actualización (versión 9.7.2) lanzada el 25 de febrero.

> *«La versión 9.7.2 de Vision and Vision Pro es una versión de mantenimiento que soluciona distintas vulnerabilidades, como el aumento de privilegios locales que envían información confidencial en texto plano»*, dijo la compañía.

Netop cuenta con la mitad de las empresas Fortune 100 entre sus clientes, y conecta a más de 3 millones de profesores y estudiantes con su software. Netop Vision Pro permite a los maestros realizar tareas de forma remota en las computadoras de los estudiantes, como monitorear y administrar sus pantallas en tiempo real, restringir el acceso a una lista de sitios web permitidos, iniciar aplicaciones e incluso redirigir la atención de los estudiantes cuando están distraídos.

En la investigación de McAfee se descubrieron varios defectos de diseño, como:

- CVE-2021-27194: Todo el tráfico de red entre el profesor y el alumno se envía sin cifrar y en texto sin cifrar, por ejemplo, credenciales de Windows y captura de pantalla, sin la capacidad de habilitarlo durante la configuración. Además, las capturas de pantalla se envían al maestro tan pronto como se conecten a un aula para permitir el monitoreo en tiempo real.
- CVE-2021-27195: Un atacante puede monitorear el tráfico no cifrado para hacerse pasar por un maestro y ejecutar código de ataque en las máquinas de los estudiantes modificando el paquete que contiene la aplicación exacta que se ejecutará, como inyectar scripts de PowerShell adicionales.
- CVE-2021-27192: Un botón de *«soporte técnico»* en el menú *«Acerca de»* de Netop se puede aprovechar para obtener una escalada de privilegios como usuario del *«sistema»* y ejecutar comandos arbitrarios, reiniciar Netop y apagar la computadora.
- CVE-2021-27193: Una falla de privilegio en el complemento de chat de Netop podría explotarse para leer y escribir archivos arbitrarios en un *«directorio de trabajo»* que se utiliza como ubicación para colocar todos los archivos enviados por el instructor. Pero aún, esta ubicación de directorio se puede cambiar de forma remota para sobrescribir cualquier archivo en la PC remota, incluidos los ejecutables del sistema.

CVE-2021-27193 también tiene una calificación de 9.5 de un máximo de 10 en el sistema de calificación CVSS.

Al explotar las vulnerabilidades, un atacante podría implementar ransomware o instalar software de registro de teclas y realizar encadenamiento de CVE-2021-27195 y CVE-2021-27193 para vigilar las cámaras web de las computadoras individuales que ejecutan el software.

Aunque la mayoría de las vulnerabilidades ya fueron solucionadas, las correcciones implementadas por Netop aún no abordan la falta de cifrado de red, que se espera sea implementado en una actualización futura.

> *«Un atacante no tiene que comprometer la red de la escuela, todo lo que necesita*

> *es encontrar cualquier red donde este software sea accesible, como una biblioteca, cafetería o red doméstica. No importa dónde se vea comprometida una de las PC de los estudiantes, ya que un malware bien diseñado podría permanecer inactivo y escanear cada red a la que se conecta la PC infectada hasta que encuentre otras instancias vulnerables de Netop Vision Pro para propagar aún más la infección»,* dijeron los investigadores Sam Quinn y Douglas McKee.
>
> *«Una vez que estas máquinas se han visto comprometidas, el atacante remoto tiene el control total del sistema, ya que heredan los privilegios del sistema. Nada en este momento podría evitar que un atacante que se ejecuta como «sistema» acceda a archivos, finalice cualquier proceso o cause estragos en la máquina comprometida»,* agregaron.

Estos hallazgos se producen en un momento en que el Buró Federal de Investigación advirtió la semana pasada sobre un momento de los ataques de ransomware PYSA, también conocido como Mespinoza, dirigidos a instituciones educativas en 12 estados de Estados Unidos y Reino Unido.