El equipo de TeamViewer lanzó recientemente una nueva versión del software, que incluye un parche para una vulnerabilidad grave (CVE-2020-13699), que de explotarse, podría permitir que atacantes remotos roben la contraseña de su sistema y eventualmente la comprometan.

Lo más preocupante al respecto es que el atacante puede operar casi de forma automática sin requerir mucha interacción con las víctimas y simplemente convenciéndolas de que visiten un sitio web malicioso una vez.

Jeffrey Hofmann, de Praetorian, fue quien descubrió la vulnerabilidad de alto riesgo, que reside en la forma en que TeamViewer cita sus controladores URI personalizados, lo que podría permitir a un atacante forzar al software a transmitir una solicitud de autenticación NTLM al sistema del atacante.

Un atacante puede aprovechar el esquema URI de TeamViewer desde una página web para engañar a la aplicación instalada en el sistema de la víctima para que inicie una conexión al recurso compartido SMB remoto propiedad del atacante.

A su vez, esto desencadena el ataque de autenticación SMB, filtra el nombre de usuario del sistema y la versión hash NTLMv2 de la contraseña a los atacantes, lo que les permite usar credenciales robadas para autenticar la computadora o los recursos de red de las víctimas.

Para aprovechar con éxito la vulnerabilidad, un atacante necesita incrustar un iframe malicioso en un sitio web y luego engañar a las víctimas para que visiten esa URL creada con fines malintencionados. Una vez que la víctima hace clic, TeamViewer iniciará automáticamente su cliente de escritorio de Windows y abrirá un recurso compartido SMB remoto.

Después, el sistema operativo Windows de la víctima *«realizará la autenticación NTLM al abrir el recurso compartido SMB y esa solicitud se puede transmitir (utilizando una herramienta como el respondedor para la ejecución del código), o capturarse para descifrar*

el hash».

La vulnerabilidad, categorizada como *«Manejador de URI sin comillas»,* afecta a los *«manejadores de URI teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocalln1, y tvVideopn1»*, dijo el investigador.

Los desarrolladores de TeamViewer corrigieron la vulnerabilidad citando los parámetros pasados por los controladores de URI afectados, por ejemplo, URL:teamviewer10 Protocol «C:\ProgramFiles(X86)\TeamViewer\TeamViewer.exe»»%1».

Aunque la vulnerabilidad no se está explotando en la naturaleza ahora, el software tiene una gran popularidad, por lo que se recomienda a los usuarios que actualicen a la versión 15.8.3, ya que solo es cuestión de tiempo para que los hackers empiecen a aprovechar la falla.