La agencia cibernética de Seguridad Nacional informó que probó un exploit funcional para la vulnerabilidad BlueKeep, capaz de lograr la ejecución remota de código en un dispositivo vulnerable.

Hasta ahora, la mayoría de las explotaciones privadas dirigidas a BlueKeep habrían desencadenado una condición de denegación de servicio, capaz de desconectar a las computadoras. Pero un exploit capaz de ejecutar código o malware de forma remota en una computadora afectada, un evento que el gobierno teme, podría desencadenar un incidente mundial como el de WannaCry en 2017.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), confirmó en una alerta el lunes que había utilizado BlueKeep para ejecutar el código de forma remota en una computadora con Windows 2000.

Windows 2000 no fue incluido en el aviso de Microsoft. Un portavoz de CISA dijo que la agencia *«se coordina con las partes interesadas externas para validar las vulnerabilidades».*

Aunque no se han lanzado ataques públicos, la alerta de CISA sirve como advertencia de que los atacantes maliciosos podrían lograr pronto los mismos resultados.

Tanto Microsoft como el gobierno federal hicieron sonar la alarma en las últimas semanas sobre los riesgos planteados por BlueKeep.

El error, conocido como CVE-2019-0708, es una vulnerabilidad crítica que afecta a las computadoras con Windows 7 y versiones anteriores, incluyendo varios sistemas operativos para servidor. La vulnerabilidad se puede utilizar para ejecutar código a nivel del sistema, incluidos sus datos. También es de tipo *«wormable»,* lo que significa que se puede propagar desde una sola computadora conectada a Internet a todos los demás dispositivos afectados en la red.

Microsoft emitió parches el mes pasado, pero hasta un millón de dispositivos siguen siendo vulnerables. Kevin Beaumont, un investigador de seguridad con sede en Reino Unido, afirmó

en un tweet que la cantidad de dispositivos afectados *«será mucho más alta»* una vez que se aprovechen los ataques de código dentro de una organización.

La agencia de Seguridad Nacional, a inicios de este mes, emitió un raro aviso, que advierte a los usuarios a parchear *«ante las crecientes amenazas»* de explotación.