Alrededor de 1 millón de sistemas Windows no se han parcheado y cuentan con vulnerabilidades relacionadas con ejecución remota de código crítico, recientemente revelada en el Protocolo de Escritorio Remoto (RDP) de Windows, dos semanas después de que Microsoft lanzara su parche de seguridad.

Si se explota, la vulnerabilidad podría permitir que un atacante cause de forma sencilla estragos en todo el mundo, potencialmente mucho peor que lo que hicieron WannaCry y NotPetya en 2017.

Apodado como BlueKeep y rastreado como CVE-2019-0708, la vulnerabilidad afecta las ediciones Windows 2003, XP, Windows 7, Windows Server 2008 y 2008 R2 y podría propagarse automáticamente en sistemas protegidos.

La vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y tomar el control de una computadora específica simplemente enviando solicitudes especialmente diseñadas al Servicio de Escritorio Remoto (RDS) del dispositivo por medio del RDP, sin necesidad de interacción alguna por parte del usuario.

Describiendo la vulnerabilidad de BlueKeep como Wormable que podría permitir que el malware se propague a los sistemas vulnerables como WannaCry, Microsoft lanzó una solución de seguridad para solucionar la vulnerabilidad con sus actualizaciones del martes.

Sin embargo, la última exploración de Internet realizada por Robert Graham, jefe de la firma de investigación de seguridad ofensiva Errata Security, reveló que aproximadamente 950,000 máquinas de acceso público en Internet son vulnerables a BlueKeep.

Esto significa que aún después de haber eliminado el parche de seguridad, no todos los usuarios y organizaciones lo han implementado para abordar el problema, lo que representa un riesgo masivo para las personas y las organizaciones, incluidos los entornos industriales y de salud.

Graham utilizó *«rdpscan»*, una herramienta de escaneo rápido que construyó sobre su

masscan port scanner, que puede escanear todo el Internet en busca de sistemas que aún son vulnerables a la BlueKeep, y encontró un total de 7 millones de sistemas que estaban escuchando en el puerto 3389, de los cuales, cerca de 1 millón de sistemas siguen siendo vulnerables.

> *«Es probable que los hackers descubran un robusto exploit el próximo mes y causen estragos en estas máquinas. Eso significa que cuando el gusano golpee, es probable que comprometa esos millones de dispositivos. Esto probablemente llevará a un evento tan dañino como WannaCry y NotPetya a partir de 2017, potencialmente peor, ya que los hackers han perfeccionado sus habilidades explotando estas cosas en busca de ransomware y otras desagradables»,* dijo el investigador.

La vulnerabilidad de BlueKeep tiene tanto potencial para causar problemas en todo el mundo que forzó a Microsoft a lanzar parches no solo para las versiones de Windows compatibles, sino también para Windows XP, Windows Vista y Windows Server 2003, que ya no reciben el soporte general de la empresa, pero que aún son ampliamente usados.

No solo investigadores, hackers malintencionados y ciberdelincuentes también comenzaron a escanear Internet en busca de sistemas vulnerables de Windows para atacarlos con malware, dijo GreyNoise Intelligence.

> *«GreyNoise está observando pruebas de barrido para sistemas vulnerables al RDP BlueKeep (CVE-2019-0708), vulnerabilidad de varias docenas de hosts en Internet. Esta actividad se ha observado exclusivamente en los nodos de salida de Tor y es probable que sea ejecutado por un solo actor»*, agregó.

Sin embargo, hasta el momento, ningún investigador de seguridad publicó ningún código de prueba de concepto para BlueKeep, aunque algunos de ellos han confirmado que han

desarrollado con éxito un exploit funcional.

Si no has podido solucionar el error con un parche, entonces puedes tomar las siguientes medidas:

- Deshabilitar los servicios RDP, si no son requeridos.
- Bloquear el puerto 3389 utilizando un firewall o hacer accesible solo por medio de una VPN privada.
- Habilitar la autenticación de nivel de red (NLA).