La Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (CISA), emitió ayer un aviso donde advierte a las organizaciones que cambien todas sus credenciales de Active Directory como defensa contra ataques cibernéticos que intentan aprovechar una vulnerabilidad conocida de ejecución remota de código (RCE), en los servidores Pulse Secure VPN, incluso si ya se han parchado.

La advertencia llegar tres meses después de otra alerta de CISA que insta a los usuarios y administradores a parchear entornos Pulse Secure VPN para frustrar los ataques de explotación de dicha vulnerabilidad.

> *«Los actores de amenazas que explotaron con éxito CVE-2019-11510 y robaron las credenciales de una organización víctima aún podrán acceder, y moverse lateralmente a la red de esa organización después de haber parcheado la vulnerabilidad si la organización no cambió las credenciales robadas»*, dijo CISA.

CISA también lanzó una herramienta para ayudar a los administradores de red a buscar cualquier indicador de compromiso asociado con la falla.

Rastreada como CVE-2019-11510, la vulnerabilidad de lectura de archivos arbitrarios previa a la autenticación podría permitir a los atacantes remotos no autenticados comprometer los servidores VPN vulnerables y obtener acceso a todos los usuarios activos y sus credenciales de texto sin formato, y ejecutar comandos arbitrarios.

La falla se debe al hecho de que el recorrido del directorio está codificado para permitirse si una ruta contiene *«dana/html5/acc»*, lo que permite que un atacante envíe URL especialmente diseñadas para leer archivos confidenciales, como *«/etc/password/»*, que contiene información acerca de cada usuario en el sistema.

Para abordar el problema, Pulse Secure lanzó un parche fuera de banda el 24 de abril de 2019. Mientras que el 24 de agosto de 2019, la empresa de inteligencia de seguridad Bad Packets pudo descubrir 14,528 servidores Pulse Secure sin parchear, un escaneo posterior a

partir del mes pasado produjo 2,099 puntos finales vulnerables, lo que indica que una gran mayoría de las organizaciones han parcheado sus puertas de enlace VPN.

El hecho de que todavía existan miles de servidores Pulse Secure VPN sin parches los ha convertido en un objetivo lucrativo para que los malos actores distribuyan malware.

Un informe de ClearSky encontró a hackers patrocinados por el estado iraní que utilizan la vulnerabilidad CVE-2019-11510, entre otros, para penetrar y robar información de empresas de TI y telecomunicaciones en todo el mundo.

Según un aviso de la NSA de octubre de 2019, el *«código de explotación está disponible gratuitamente en línea por medio del marco Metasploit, así como GitHub. Los ciberdelincuentes maliciosos están utilizando activamente este código de explotación».*

En una alerta similar emitida el año pasado, el Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unido, se advirtió que los grupos de amenazas avanzadas están explotando la vulnerabilidad para atacar a organizaciones gubernamentales, militares, académicas, comerciales y de atención médica.

Recientemente, Travelex, la firma de cambio de moneda extranjera y seguro de viaje, se convirtió en una víctima después de que piratas informáticos sembraron el ransomware Sodinokibi en las redes de la compañía a través de la vulnerabilidad de Pulse Secure.

Aunque los operadores de ransomware exigieron un rescate de 6 millones de dólares, un informe del Wall Street Journal dijo la semana pasada que la compañía pagó 2.3 millones de dólares en Bitcoin para resolver el problema.

Debido a esto, las organizaciones deben actualizar su VPN Pulse Secure, restablecer las credenciales y buscar solicitudes de registro no autenticadas e intentos de explotación.

CISA también sugirió eliminar los programas de acceso remoto no aprobados e inspeccionar las tareas programadas en busca de scripts o ejecutables que puedan permitir que un

atacante se conecte a un entorno.