Microsoft está solicitando a los clientes mantener actualizados sus servidores de Exchange y tomar medidas para reforzar el entorno, como habilitar Windows Extended Protection y configurar la firma basada en certificados de las cargas útiles de serialización de PowerShell.

> *«Los atacantes que buscan explotar los servidores de Exchange sin parches no van a desaparecer. Hay demasiados aspectos de los entornos de Exchange locales sin parches que son valiosos para los hackers que buscan filtrar datos o cometer otros actos maliciosos»,* dijo el equipo de Exchange de Microsoft.

Microsoft también enfatizó que las mitigaciones emitidas por la compañía son solo una solución provisional y que pueden *«volverse insuficientes para proteger contra todas las variaciones de un ataque»*, lo que requiere que los usuarios instalen las actualizaciones de seguridad necesarias para proteger los servidores.

Se ha demostrado que Exchange Server es un vector de ataque lucrativo en los últimos años, con una serie de fallas de seguridad en el software armado como día cero para hackear sistemas.

Solo en los últimos dos años, se han descubierto varios conjuntos de vulnerabilidades en Exchange Server, incluidos ProxyLogon, ProxyOracle, ProxyShell, ProxyToken, ProxyNotShell y un bypass de mitigación de ProxyNotShell conocido como OWASSRF, algunos de los cuales han sido objeto de una explotación generalizada en la naturaleza.

Bit defender, por su parte, publicó un aviso técnico en el que describió a Exchange como un *«objetivo ideal»,* a la vez que describió algunos de los ataques del mundo real que involucran las cadenas de exploits ProxyNotShell/OWASSRF desde finales de noviembre de 2022.

> *«Existe una red compleja de servicios frontend y backend, con código heredado para proporcionar compatibilidad con versiones anteriores. Los servicios de back-end confían en las solicitudes de la capa de front-end»,* dijo Martin Zugec, de Bitdefender.

Otra razón es el hecho de que varios servicios de back-end se ejecutan como Exchange Server, que cuenta con privilegios de SYSTEM, y que los exploits podrían otorgar al atacante acceso malicioso al servicio remoto de PowerShell, allanando el camino para la ejecución de comandos maliciosos.

Con ese fin, los ataques que utilizan las fallas de ProxyNotShell y OWASSRF como armas se han dirigido a las industrias de artes y entretenimiento, consultoría, derecho, fabricación, bienes raíces y venta al por mayor ubicadas en Austria, Kuwuait, Polonia, Turquía y Estados Unidos.

> *«Estos tipos de ataques de falsificación de solicitudes del lado del servidor (SSRF) permiten que un atacante envíe una solicitud diseñada desde un servidor vulnerable a otros servidores para acceder a recursos o información a los que de otro modo no se puede acceder de forma directa»,* dijo la compañía.

La mayoría de los ataques son oportunistas y no enfocados o dirigidos, y las infecciones culminan en el intento de implementación de shells web y software de administración y monitoreo remoto (RMM) como ConnectWise Control y GoTo Resolve.

Los shells web no solo ofrecen un mecanismo de acceso remoto persistente, sino que también permiten a los delincuentes realizar una amplia gama de actividades de seguimiento e incluso, vender el acceso a otros grupos de hackers para obtener ganancias.

En algunos casos, los servidores de prueba usados para alojar cargas útiles se vieron comprometidos por los propios servidores de Microsoft Exchange, lo que sugiere que es

posible que se haya aplicado la misma técnica para expandir la escala de los ataques.

También se observaron esfuerzos fallidos realizados por los atacantes para descargar Cobalt Strike, así como un implante basado en Go, con nombre en código GoBackClient, que cuenta con capacidades para recopilar información del sistema y generar shells inversos.

El abuso de las vulnerabilidades de Microsoft Exchange también ha sido una táctica recurrente empleada por UNC2596 (también conocido como Tropical Scorpius), los operadores del ransomware Cuba (también conocido como COLDDRAW), con un ataque que aprovecha la secuencia de explotación de ProxyNotShell para eliminar el programa de descarga BUGHATCH.

> *«Aunque el vector de infección inicial sigue evolucionando y los atacantes aprovechan rápidamente cualquier nueva oportunidad, sus actividades posteriores a la explotación son familiares. La mejor protección contra los ciberataques modernos es una arquitectura de defensa en profundidad»,* dijo Zugec.