Los detalles técnicos han sido revelados sobre dos vulnerabilidades de seguridad en Microsoft Windows que ya han sido corregidas y que podrían ser conectadas por delincuentes cibernéticos para lograr la ejecución remota de código en el servicio de correo electrónico Outlook sin necesidad de interacción por parte del usuario.

> *«Un individuo malintencionado en la red podría combinar ambas vulnerabilidades para desarrollar un ataque de ejecución de código remoto contra clientes de Outlook sin requerir ninguna interacción por parte del usuario»,* mencionó Ben Barnea, investigador de seguridad de Akamai, quien identificó estas vulnerabilidades, en un informe compartido con The Hacker News.

Estos problemas de seguridad, que Microsoft abordó en agosto y octubre de 2023, respectivamente, se detallan a continuación:

- CVE-2023-35384 (índice CVSS: 5.4) – Falla de Bypass en la Función de Seguridad de Plataformas HTML de Windows.
- CVE-2023-36710 (índice CVSS: 7.8) – Vulnerabilidad de Ejecución Remota de Código en el Núcleo de Media Foundation de Windows.

Akamai ha identificado CVE-2023-35384 como una forma de evadir una grave vulnerabilidad de seguridad que Microsoft había solucionado en marzo de 2023. Denominada como CVE-2023-23397 (índice CVSS: 9.8), esta vulnerabilidad se relaciona con una situación donde un atacante podría elevar sus privilegios, lo que podría llevar al robo de credenciales NTLM y permitir una maniobra de ataque de relay.

Recientemente, Microsoft, junto con Proofpoint y Palo Alto Networks Unit 42, informó que un grupo de ciberespionaje ruso conocido como APT29 estaba utilizando activamente este error para obtener acceso indebido a las cuentas de las víctimas en servidores Exchange.

Es importante mencionar que CVE-2023-35384 marca el segundo bypass después de CVE-2023-29324, otro error identificado por Barnea y solucionado por Microsoft en sus

actualizaciones de seguridad de mayo de 2023.

> Barnea señaló: *«Detectamos otro método para evadir la vulnerabilidad original de Outlook, que nos permitió redirigir al cliente a un servidor manejado por el atacante y descargar un archivo de sonido dañino».*

CVE-2023-35384, al igual que CVE-2023-29324, se fundamenta en la interpretación de una dirección por la función MapUrlToZone, que podría ser aprovechada al enviar un correo que incluya un archivo sospechoso o un enlace malicioso a un usuario de Outlook.

> Microsoft advirtió: *«Existe un riesgo de evasión de seguridad cuando la plataforma MSHTML no verifica adecuadamente la Zona de Seguridad correcta para determinadas direcciones URL, lo que podría permitir a un atacante dirigir a un usuario hacia una Zona de Seguridad de Internet menos segura».*

Esta vulnerabilidad no solo podría facilitar el robo de credenciales NTLM, sino que también podría combinarse con el problema de procesamiento de sonido (CVE-2023-36710) para descargar un archivo de audio específico que, al ser reproducido en el recordatorio de Outlook, podría resultar en la ejecución de código en el dispositivo afectado.

CVE-2023-36710 afecta al componente Audio Compression Manager (ACM), una herramienta de audio de Windows, y se debe a una falla relacionada con el manejo incorrecto de datos al reproducir ciertos archivos.

> Barnea detalló: *«Finalmente, logramos explotar la falla utilizando el codec IMA ADP. El archivo tiene un tamaño cercano a 1.8 GB. Tras hacer algunas pruebas matemáticas, determinamos que el tamaño mínimo del archivo con el codec IMA ADP es de 1 GB».*

Para reducir los peligros, se sugiere que las empresas implementen medidas para bloquear conexiones no autorizadas a direcciones IP públicas. También es aconsejable desactivar ciertas funciones o restringir ciertos mecanismos de autenticación para mejorar la seguridad.