Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVO BUG CRÍTICO DE RCE EN MICROSOFT OUTLOOK ES TRIVIAL DE EXPLOTAR

15 / 02 / 2024

CONTENIDO

INTRODUCCIÓN

Una nueva vulnerabilidad crítica ha sido descubierta, poniendo en peligro la seguridad de millones de usuarios en todo el mundo. En este informe, exploraremos cómo este bug, identificado como CVE-2024-21413 y descubierto por el investigador de Check Point Haifei Li, permite a los atacantes ejecutar código malicioso de forma remota, evadiendo incluso las protecciones integradas de Outlook. Este hallazgo plantea serias preocupaciones de seguridad y destaca la importancia de aplicar los parches de seguridad de inmediato para protegerse contra posibles ataques.

NUEVO BUG CRÍTICO DE RCE EN MICROSOFT OUTLOOK ES TRIVIAL DE EXPLOTAR

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_02_15_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	15/02/2024
Es día cero (0 day):	Sí

RESUMEN

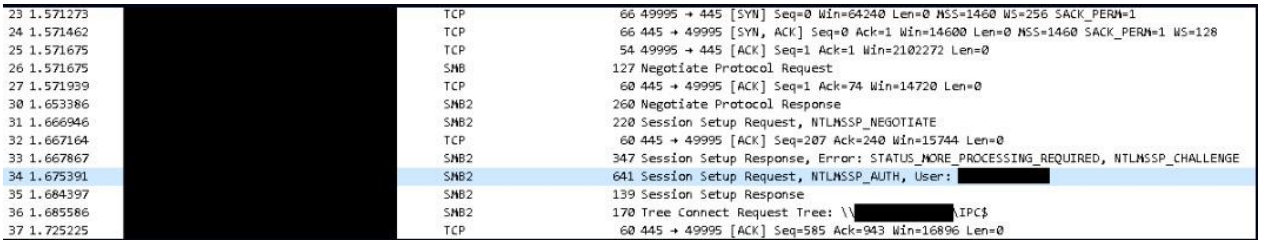
Microsoft ha advertido que los atacantes remotos no autenticados pueden explotar de manera trivial una vulnerabilidad crítica de seguridad en Outlook que también les permite evadir la Vista Protegida de Office. Descubierto por el investigador de vulnerabilidades de Check Point, Haifei Li y rastreado como CVE-2024-21413, este bug conduce a la ejecución remota de código (RCE) al abrir correos electrónicos con enlaces maliciosos utilizando una versión vulnerable de Microsoft Outlook.

Esto sucede porque la falla también permite a los atacantes evadir la Vista Protegida (diseñada para bloquear contenido dañino incrustado en archivos de Office abriéndolos en modo de solo lectura) y abrir archivos de Office maliciosos en modo de edición.

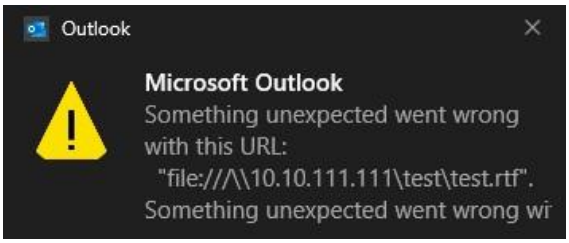
Redmond también advirtió que el Panel de Vista Previa es un vector de ataque para esta falla de seguridad, permitiendo una explotación exitosa incluso al previsualizar documentos de Office manipulados maliciosamente.

Los atacantes no autenticados pueden explotar CVE-2024-21413 de forma remota en ataques de baja complejidad que no requieren interacción del usuario.
"Un atacante que explotara con éxito esta vulnerabilidad podría obtener altos privilegios, que incluyen funcionalidades de lectura, escritura y eliminación", explica Microsoft.

"Un atacante podría crear un enlace malicioso que evita el Protocolo de Vista Protegida, lo que lleva a la filtración de información de credenciales NTLM locales y la ejecución remota de código (RCE)."



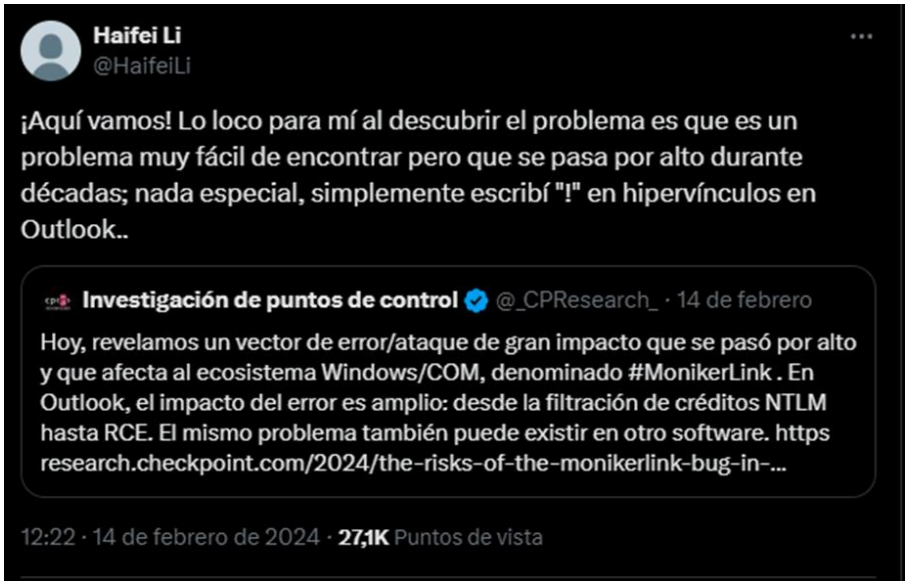
CVE-2024-21413 afecta a varios productos de Office, incluidos Microsoft Office LTSC 2021 y Microsoft 365 Apps for Enterprise, así como Microsoft Outlook 2016 y Microsoft Office 2019 (bajo soporte extendido).
Como explicó Check Point en un informe publicado hoy, la vulnerabilidad que ellos llamaron Moniker Link permite a los atacantes evadir las protecciones integradas de Outlook para enlaces maliciosos incrustados en correos electrónicos que utilizan el protocolo file:// y agregan un signo de exclamación a las URL que apuntan a servidores controlados por el atacante.



El signo de exclamación se agrega justo después de la extensión del documento, junto con un texto aleatorio (en su ejemplo, Check Point usó "algo"), como se muestra a continuación:

CLICK ME

Este tipo de hipervínculo evade la restricción de seguridad de Outlook, y Outlook accederá al recurso remoto "\\10.10.111.111\test\test.rtf" cuando se haga clic en el enlace sin mostrar advertencias ni errores.



El fallo se introdujo debido a la API insegura MkParseDisplayName, por lo que la vulnerabilidad también puede afectar a otro software que la utilicen.
El impacto de los ataques que explotan con éxito CVE-2024-21413 incluye el robo de información de credenciales NTLM, ejecución de código arbitrario a través de documentos de Office manipulados maliciosamente

"Hemos confirmado este bug/vector de ataque #MonikerLink en los entornos más recientes de Windows 10/11 + Microsoft 365 (Office 2021)," dijo Check Point.

"Es probable que otras ediciones/versiones de Office también estén afectadas. De hecho, creemos que este es un problema pasado por alto que ha existido en el ecosistema de Windows/COM durante décadas, ya que se encuentra en el núcleo de las API de COM. Recomendamos encarecidamente que todos los usuarios de Outlook apliquen el parche oficial lo antes posible."

Microsoft actualizó hoy la advertencia de seguridad CVE-2024-21413 para informar que este bug de Outlook también estaba siendo explotado en ataques como un zero-day antes del Patch Tuesday de este mes.

NOTICIA COMPLETA

https://devel.group/blog/nuevo-bug-critico-de-rce-en-microsoft-outlook-es-trivial-de-explotar/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente