Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

OUTLOOK EN RIESGO: CISA ADVIERTE SOBRE EXPLOTACIÓN ACTIVA DE FALLA CRÍTICA

07 / 02 / 2025

CONTENIDO

INTRODUCCIÓN

Se aborda un caso de intrusión cibernética que comenzó con un acceso no autorizado a un host RDP expuesto, utilizando credenciales legítimas de la cuenta de Administrador predeterminada. Lo destacado de este ataque radica en la ausencia de intentos de fuerza bruta, sugiriendo la posibilidad de acceso previo recurrente o la intervención de un intermediario de acceso. Una vez dentro, los perpetradores desplegaron diversas herramientas, incluyendo scripts por lotes, ejecutables y SoftPerfect Netscan, para realizar escaneos de red, identificar comparticiones y explorar documentos. La intrusión avanzó con movimientos laterales, deshabilitación de Windows Defender y exfiltración de datos hacia Mega.io mediante Rclone. La sorpresa llegó cuando, tras una desconexión, los atacantes se reconectaron desde una dirección IP diferente, indicando un conocimiento profundo de la red.

RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

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

ID de alerta:	DSOC-CERT_2025_02_07_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	07/02/2025
Es día cero (0 day):	No

RESUMEN

Recientemente, se ha descubierto una falla crítica en Microsoft Outlook que está siendo activamente explotada por atacantes. Esta vulnerabilidad permite la ejecución remota de código (RCE), lo que significa que un ciberdelincuente puede tomar control de un sistema sin necesidad de que el usuario abra o interactúe con un correo malicioso.
Dado que Outlook es ampliamente utilizado por empresas y usuarios para la gestión de correos electrónicos, esta vulnerabilidad representa un riesgo significativo. Microsoft ha confirmado la explotación activa de esta falla, por lo que se recomienda tomar medidas inmediatas para mitigar el impacto.

¿Qué pasó?

Investigadores en ciberseguridad han identificado una vulnerabilidad en Microsoft Outlook que permite la ejecución remota de código sin requerir interacción del usuario. Microsoft ha reconocido el problema y ha advertido que atacantes ya están explotando esta falla.
Esta vulnerabilidad es particularmente grave porque afecta a una de las herramientas de comunicación más utilizadas en el mundo, lo que amplía la superficie de ataque y aumenta la posibilidad de que organizaciones enteras sean comprometidas. Además, se ha identificado que CVE-2024-21413 afecta a varios productos de Office, incluidos Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Microsoft Outlook 2016 y Microsoft Office 2019. Los ataques exitosos pueden resultar en el robo de credenciales NTLM y la ejecución de código arbitrario a través de documentos de Office maliciosos.
La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ha emitido una alerta sobre esta vulnerabilidad debido a la detección de explotación activa en entornos reales. Se insta a las organizaciones a aplicar parches de seguridad de inmediato y reforzar sus medidas de protección.
CISA ha indicado que ha observado múltiples incidentes en los que actores maliciosos han utilizado esta vulnerabilidad para comprometer sistemas gubernamentales y empresariales en diversas industrias. Además, advierte que los atacantes están empleando técnicas avanzadas para evadir detección y mantener persistencia en los sistemas comprometidos. La agencia recomienda a todas las organizaciones implementar estrategias de monitoreo continuo y aplicar parches sin demora.

¿Cómo sucede el ataque?

El exploit aprovecha cómo Outlook procesa ciertos elementos dentro de los correos electrónicos. Un atacante puede diseñar un mensaje específico que, al ser procesado por el cliente de correo, activa la vulnerabilidad sin necesidad de que el usuario haga clic o interactúe con el contenido. Esto diferencia este ataque de otros tradicionales, como el phishing, que requieren la acción de la víctima.
Esta falla de seguridad permite a los atacantes esquivar las protecciones integradas de Outlook, habilitando la ejecución de enlaces maliciosos. Utilizando el protocolo file:// y **agregando un signo de exclamación** en las URL que apuntan a servidores controlados por el atacante.

La ejecución remota de código (RCE) se produce cuando el atacante ejecuta comandos en el sistema vulnerable de la víctima sin necesidad de autorización o interacción. En este caso, el correo malicioso se procesa automáticamente, lo que permite que el código se ejecute en el sistema sin intervención del

usuario. El atacante explota una debilidad en cómo Outlook interpreta ciertos datos dentro del correo, lo que le permite ejecutar comandos con los mismos privilegios del usuario afectado, facilitando la instalación de malware, el robo de datos o el acceso no autorizado.

¿Cuáles son las consecuencias?

- **Compromiso del sistema**: Un atacante puede ejecutar comandos en la máquina afectada, permitiéndole instalar malware, modificar archivos o crear puertas traseras para acceso futuro.
- **Robo de credenciales**: La explotación de esta falla puede permitir a los atacantes extraer datos sensibles, como credenciales almacenadas o información financiera.
- **Movimientos laterales en redes empresariales**: Una vez comprometido un equipo, el atacante puede extender su acceso a otros sistemas dentro de la red, aumentando el alcance del ataque.
- **Posibles ataques de ransomware**: La ejecución remota de código puede ser utilizada para desplegar ransomware y cifrar archivos, bloqueando el acceso a información crítica hasta que se pague un rescate.

Lección aprendida

Esta vulnerabilidad en Microsoft Outlook deja en evidencia la importancia de mantener un enfoque proactivo en la ciberseguridad. La explotación de fallas sin necesidad de interacción del usuario demuestra que confiar únicamente en la prudencia de los empleados no es suficiente para evitar ataques. Es fundamental adoptar estrategias de defensa en profundidad. Además, refuerza la necesidad de que las organizaciones implementen políticas de seguridad que reduzcan la exposición a amenazas emergentes y minimicen el impacto de posibles ataques.

Recomendaciones

1. **Aplicar actualizaciones de seguridad:** Microsoft ha lanzado parches de seguridad para abordar esta vulnerabilidad. Se recomienda actualizar Outlook y otros productos de Microsoft lo antes posible para evitar la explotación activa de la falla.
2. **Configurar reglas de filtrado en correos electrónicos:** Las organizaciones pueden implementar reglas en sus servidores de correo para bloquear o filtrar mensajes sospechosos que contengan elementos potencialmente maliciosos.
3. **Restringir la ejecución de código en entornos vulnerables:** Se pueden aplicar controles de ejecución de código restringida, como reglas en Microsoft Defender o políticas de grupo, para evitar que procesos maliciosos se ejecuten automáticamente.
4. **Monitorear y analizar tráfico sospechoso:** El monitoreo de actividad inusual en los dispositivos y la red puede ayudar a identificar intentos de explotación. Se recomienda el uso de herramientas de detección de amenazas para analizar comportamientos anómalos.
5. **Educar a los usuarios sobre ciberseguridad:** Capacitar a los empleados en buenas prácticas de seguridad, como la identificación de correos sospechosos y el uso de herramientas seguras, puede reducir el impacto de este tipo de ataques.

NOTICIA COMPLETA

https://devel.group/blog/outlook-en-riesgo-cisa-advierte-sobre-explotacion-activa-de-falla-critica/

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