Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD ZERO-CLICK EN WINDOWS OLE: UNA AMENAZA SILENCIOSA PARA LOS USUARIOS

04 / 02 / 2025

CONTENIDO

INTRODUCCIÓN

Las vulnerabilidades Zero-Click representan un riesgo significativo en el ámbito de la ciberseguridad, ya que permiten a los atacantes comprometer un sistema sin que la víctima realice ninguna acción, como hacer clic en enlaces o descargar archivos sospechosos. Recientemente, se ha descubierto una falla crítica en Windows OLE, una tecnología clave en el ecosistema de Microsoft que facilita la integración de contenido entre aplicaciones. Esta vulnerabilidad expone a millones de usuarios y organizaciones, permitiendo la ejecución remota de código malicioso con solo previsualizar un archivo manipulado. Su gravedad radica en que los ciberdelincuentes pueden aprovecharla para tomar el control de dispositivos, robar información sensible e incluso propagar ataques dentro de redes corporativas sin dejar rastro evidente.

VULNERABILIDAD ZERO-CLICK EN WINDOWS OLE: UNA AMENAZA SILENCIOSA PARA LOS USUARIOS

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

ID de alerta:	DSOC-CERT_2025_02_04_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	04/02/2025
Es día cero (0 day):	No

RESUMEN

Las vulnerabilidades Zero-Click representan una amenaza significante en la ciberseguridad, ya que permiten la explotación de sistemas sin necesidad de interacción por parte del usuario. Recientemente, se ha descubierto una falla crítica en Windows OLE (Object Linking and Embedding), una tecnología fundamental en el ecosistema de Microsoft que permite la integración de contenido entre aplicaciones, como la inserción de hojas de cálculo en documentos de Word o la apertura de enlaces embebidos en correos electrónicos.

Esta vulnerabilidad deja expuestos a millones de usuarios y organizaciones, ya que los atacantes pueden aprovecharse de ella para ejecutar código malicioso en sistemas afectados sin requerir que la víctima haga clic en ningún enlace o descargue archivos sospechosos. Su gravedad radica en la posibilidad de que los ciberdelincuentes obtengan acceso total a un dispositivo con solo enviar un documento manipulado o aprovechar la vista previa en ciertos servicios.

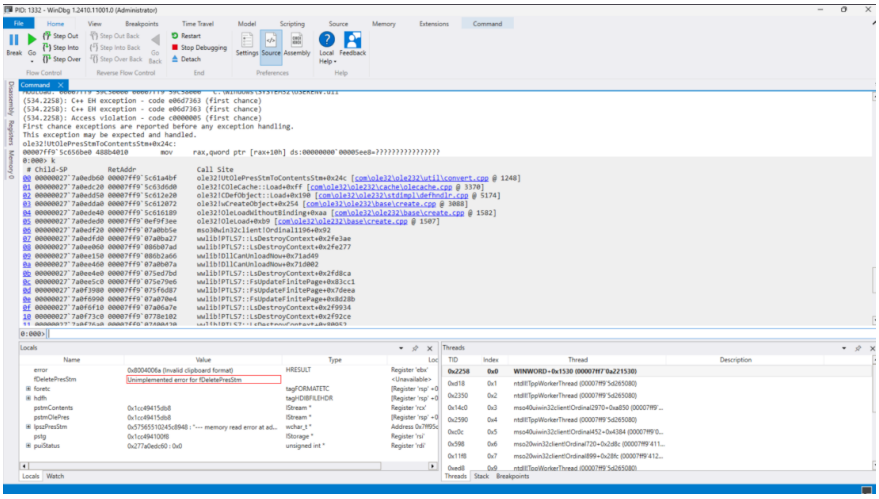
¿Qué es esta vulnerabilidad?

Se ha identificado una vulnerabilidad crítica en Windows OLE con la identificación CVE-2025-21298, que permite a los atacantes ejecutar código malicioso en un sistema sin requerir interacción del usuario. Esta vulnerabilidad, clasificada como Zero-Click, permite explotar archivos con contenido embebido para comprometer sistemas de manera sigilosa. Microsoft ha anunciado que los sistemas operativos afectados incluyen: Windows 10, 11, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 y 2025, lo que amplía el alcance del problema y afecta a una gran cantidad de usuarios y organizaciones.

La gravedad de esta vulnerabilidad ha sido evaluada con un puntaje de 9.8 en la CVSS, lo que la coloca en la categoría de crítica, indicando su alto potencial de explotación.

¿Cómo sucede el ataque?

Los atacantes pueden aprovechar esta vulnerabilidad enviando documentos de Microsoft Office o archivos manipulados que explotan un fallo en OLE. Cuando el sistema intenta procesar estos archivos, ya sea en una vista previa o al abrirlos, se ejecuta código malicioso en segundo plano sin que la víctima lo note. Esto facilita la instalación de malware, robo de información o incluso el control remoto del sistema.



Para visualizar la PoC, basta con abrir el archivo "poc.rtf" publicado en nuestro repositorio de GitHub y observar cómo Microsoft Word se bloquea inmediatamente. Este comportamiento demuestra el impacto de la vulnerabilidad y su facilidad de explotación.

¿Por qué es peligrosa esta vulnerabilidad?

- No requiere interacción del usuario: Puede ejecutarse de forma automática sin que la víctima haga clic en nada.
- Afecta a una tecnología ampliamente utilizada: Windows OLE está presente en múltiples aplicaciones y versiones de Windows.
- Posibilidad de ejecución remota de código: Un atacante puede tomar control del dispositivo afectado, desplegar ransomware, robar datos sensibles o incluso atacar otras máquinas dentro de la misma red.

Conclusión

La vulnerabilidad Zero-Click en Windows OLE representa una grave amenaza para la seguridad de sistemas en todo el mundo. Esta falla permite a los atacantes ejecutar código malicioso de manera remota, sin que el usuario tenga que interactuar con el sistema. La vulnerabilidad es especialmente peligrosa porque no requiere ninguna acción por parte de la víctima y puede ser explotada a través de archivos comunes, como documentos de Office. Las organizaciones y usuarios deben estar conscientes de este riesgo y tomar medidas inmediatas para mitigar su impacto.

Recomendaciones y Mitigación

Para proteger los sistemas de esta vulnerabilidad Zero-Click en Windows OLE, se recomienda tomar las siguientes medidas:

1. Actualizar a las últimas versiones de software: Asegúrate de que todos los sistemas operativos y aplicaciones de Microsoft, especialmente aquellos que utilizan Windows OLE, estén

actualizados con los parches de seguridad más recientes. Las actualizaciones de seguridad lanzadas por Microsoft corrigen vulnerabilidades críticas como esta.

2. Desactivar las vistas previas de archivos: Desactivar la opción de vista previa de archivos en aplicaciones como Microsoft Outlook y Windows Explorer puede ayudar a prevenir la explotación de esta vulnerabilidad. Esto evitará que los atacantes puedan ejecutar código malicioso cuando se visualicen documentos manipulados.
3. Implementar soluciones de seguridad avanzadas: Utiliza herramientas de detección de amenazas y antivirus que puedan identificar comportamientos sospechosos o ataques que intenten explotar vulnerabilidades Zero-Click.
4. Educar a los usuarios: Aunque esta vulnerabilidad no requiere interacción, la educación sobre el manejo seguro de correos electrónicos y archivos sigue siendo crucial para prevenir otros tipos de ataques, como el phishing o la descarga de malware.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-zero-click-en-windows-ole-una-amenaza-silenciosa-para-los-usuarios/

CONTACTOS DE SOPORTE

Correo electrónico: info@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/