Nro. Alerta:	AL-2025-006	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	07-feb-2025	Vulnerabilidad de ejecución remota de código OLE de Windows	Pág.: **1** of **8**

I. DATOS GENERALES

Clase de alerta: Vulnerabilidad

Tipo de vulnerabilidad: Vulnerabilidad de ejecución remota de código OLE de Windows - CVE-2025-21298

Nivel de riesgo: Alta

II. ALERTA

Figura 1.- CVE-2025-21298: Una vulnerabilidad crítica de Windows OLE Zero-Click

CVSS:

Score	Severity	Version	Vector String
9.8	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Figura 2.- CVSS Vulnerabilidad de ejecución remota de código OLE de Windows - CVE-2025-21298

III. INTRODUCCIÓN

La vulnerabilidad crítica CVE-2025-21298 se encuentra presente en el OLE (Object Linking and Embedding) de Windows que permite la ejecución remota de código, permite incrustar y vincular documentos y otros objetos; esta vulnerabilidad, con una puntuación CVSS de 9,8, permite la ejecución remota de código (RCE) a través de

correos electrónicos especialmente diseñados, lo que supone importantes riesgos para los usuarios y las organizaciones. OLE es una tecnología patentada desarrollada por Microsoft que permite incrustar y vincular documentos y objetos.

Esta vulnerabilidad es explotada por los atacantes a través de correos electrónicos especialmente diseñados enviados a los usuarios de Microsoft Outlook. La falla se puede desencadenar enviando la carga útil (payload) inicial por ejemplo documento RTF que está incrustado con el código malicioso. El simple hecho de abrir o de obtener una vista previa del documento malicioso puede desencadenar la ejecución de código arbitrario en el sistema de la víctima, lo que resulta en la descarga de la carga útil de alto perfil que potencialmente otorga al atacante un control no autorizado. Esta es una amenaza importante para las organizaciones, ya que los atacantes normalmente desencadenan esta vulnerabilidad mediante la elaboración de correos electrónicos de phishing y atraen a las víctimas para que hagan clic en el archivo adjunto.

Al abrir con éxito el documento malicioso, ejecuta un comando de PowerShell en segundo plano que descarga una carga útil en el sistema de la víctima que, en última instancia, proporciona el control al atacante.

IV. VECTOR DE ATAQUE

Los atacantes pueden explotar esta falla enviando un correo electrónico malicioso que contenga un documento RTF dañino.

Cuando la víctima abre o previsualiza el correo electrónico en Microsoft Outlook, se desencadena la vulnerabilidad, lo que permite al atacante ejecutar código arbitrario en el sistema afectado.

V. IMPACTO

Tras una explotación exitosa, los atacantes pueden obtener los mismos privilegios que el usuario actual, lo que puede llevar a un compromiso completo del sistema.

Esto incluye la capacidad de:

- Instalar programas
- Ver, cambiar o eliminar datos
- Crear nuevas cuentas con todos los derechos de usuario

La naturaleza de cero clics de esta vulnerabilidad significa que la explotación puede ocurrir sin ninguna interacción del usuario más allá de abrir o previsualizar el correo electrónico malicioso, lo que aumenta inherentemente su gravedad.

CVE-2025-21298 representa una amenaza de seguridad significativa debido a su alta gravedad y al potencial de ejecución remota de código sin interacción del usuario.

La acción inmediata a través de la aplicación de parches y la implementación de soluciones alternativas recomendadas es esencial para proteger los sistemas de posibles explotaciones. La supervisión continua y el uso de reglas de detección pueden mejorar aún más la defensa de una organización contra dichas vulnerabilidades.

VI. INDICADORES DE COMPROMISO

La vulnerabilidad reside en la biblioteca ole32.dll, específicamente dentro de la función 'UtOlePresStmToContentsStm'. Esta función es responsable de convertir los datos en un flujo "OlePres" dentro de un almacenamiento OLE en datos con el formato adecuado e insertarlos en el flujo "CONTENTS" en el mismo almacenamiento.

Fuente CVSS: Microsoft
Cadena vectorial: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Métrica: CVSS:3.1 9.8 / 8.5

Vendedor	Producto	Plataformas	Afectación
Microsoft	Windows 10, versión 1809	Sistemas de 32 bits, sistemas basados en x64	Afectado desde **10.0.17763.0** antes de **10.0.17763.6775**

Vendedor	Producto	Plataformas	Afectación
Microsoft	Windows Server 2019	Sistemas basados en x64	Afectado desde 10.0.17763.0 antes de 10.0.17763.6775
Microsoft	Windows Server 2019 (instalación de Server Core)	Sistemas basados en x64	Afectado desde 10.0.17763.0 antes de 10.0.17763.6775
Microsoft	Windows Server 2022	Sistemas basados en x64	Afectado desde 10.0.20348.0 hasta 10.0.20348.3091
Microsoft	Windows 10 versión 21H2	Sistemas de 32 bits, sistemas basados en ARM64, sistemas basados en x64	Afectado desde 10.0.19043.0 antes de 10.0.19044.5371
Microsoft	Windows 11 versión 22H2	Sistemas basados en ARM64, sistemas basados en x64	Afectado desde 10.0.22621.0 antes de 10.0.22621.4751
Microsoft	Windows 10, versión 22H2	Sistemas basados en x64, sistemas basados en ARM64, sistemas de 32 bits	Afectado desde 10.0.19045.0 antes de 10.0.19045.5371
Microsoft	Windows Server 2025 (instalación de Server Core)	Sistemas basados en x64	Afectado desde 10.0.26100.0 antes de 10.0.26100.2894
Microsoft	Windows 11 versión 22H3	Sistemas basados en ARM64	Afectado desde 10.0.22631.0 antes de 10.0.22631.4751
Microsoft	Windows 11 versión 23H2	Sistemas basados en x64	Afectado desde 10.0.22631.0 antes de 10.0.22631.4751

Vendedor	Producto	Plataformas	Afectación
Microsoft	Windows Server 2022, edición 23H2 (instalación de Server Core)	Sistemas basados en x64	Afectado desde 10.0.25398.0 antes de 10.0.25398.1369
Microsoft	Windows 11 versión 24H2	Sistemas basados en ARM64, sistemas basados en x64	Afectado desde 10.0.26100.0 antes de 10.0.26100.2894
Microsoft	Windows Server 2025	Sistemas basados en x64	Afectado desde 10.0.26100.0 antes de 10.0.26100.2894
Microsoft	Windows 10 versión 1507	Sistemas de 32 bits, sistemas basados en x64	Afectado desde 10.0.10240.0 antes de 10.0.10240.20890
Microsoft	Windows 10, versión 1607	Sistemas de 32 bits, sistemas basados en x64	Afectado desde 10.0.14393.0 antes de 10.0.14393.7699
Microsoft	Windows Server 2016	Sistemas basados en x64	Afectado desde 10.0.14393.0 antes de 10.0.14393.7699
Microsoft	Windows Server 2016 (instalación de Server Core)	Sistemas basados en x64	Afectado desde 10.0.14393.0 antes de 10.0.14393.7699
Microsoft	Windows Server 2008 Service Pack 2	Sistemas de 32 bits	Afectado desde 6.0.6003.0 antes de 6.0.6003.23070

Vendedor	Producto	Plataformas	Afectación
Microsoft	Windows Server 2008 Service Pack 2 (instalación de Server Core)	Sistemas de 32 bits, sistemas basados en x64	Afectado desde 6.0.6003.0 antes de 6.0.6003.23070
Microsoft	Windows Server 2008 Service Pack 2	Sistemas basados en x64	Afectado desde 6.0.6003.0 antes de 6.0.6003.23070
Microsoft	Windows Server 2008 R2 Service Pack 1	Sistemas basados en x64	Afectado desde 6.1.7601.0 antes de 6.1.7601.27520
Microsoft	Windows Server 2008 R2 Service Pack 1 (instalación de Server Core)	Sistemas basados en x64	Afectado desde 6.1.7601.0 antes de 6.1.7601.27520
Microsoft	Windows Server 2012	Sistemas basados en x64	Afectado desde 6.2.9200.0 antes de 6.2.9200.25273
Microsoft	Windows Server 2012 (instalación de Server Core)	Sistemas basados en x64	Afectado desde 6.2.9200.0 antes de 6.2.9200.25273
Microsoft	Windows Server 2012 R2	Sistemas basados en x64	Afectado desde 6.3.9600.0 antes de 6.3.9600.22371
Microsoft	Windows Server 2012 R2 (instalación de Server Core)	Sistemas basados en x64	Afectado desde 6.3.9600.0 antes de 6.3.9600.22371

VII. RECOMENDACIONES

- Leer mensajes de correo electrónico en texto sin formato: la configuración de Microsoft Outlook para mostrar los mensajes de correo electrónico en texto sin formato reduce el riesgo de desencadenar objetos OLE malintencionados. Sin embargo, este enfoque afectará a la legibilidad del correo electrónico porque el contenido de texto enriquecido, como imágenes y fuentes especiales, ya no se mostrará correctamente. Para obtener más información, consulte la documentación de Microsoft.

- Evite abrir archivos RTF de fuentes no confiables: Los usuarios deben tener cuidado con los correos electrónicos que contienen archivos adjuntos o contenido RTF, especialmente de remitentes desconocidos.

- Aplique el principio de mínimo privilegio: restrinja los privilegios de los usuarios ara reducir el impacto de los exploits exitosos.

- Microsoft ha lanzado parches para abordar esta vulnerabilidad como parte de sus actualizaciones; se recomienda a los usuarios y a las organizaciones que apliquen estas actualizaciones con prontitud para mitigar los riesgos potenciales.

- Para aquellos que no pueden actualizar inmediatamente, una solución alternativa recomendada es configurar Outlook para leer todo el correo estándar en formato de texto sin formato, lo que reduce el riesgo de explotación automática.

- Los profesionales de seguridad pueden utilizar reglas de detección para identificar intentos de explotación de CVE-2025-21298: por ejemplo, las reglas Sigma están disponibles para detectar sistemas que interactúan con tipos de archivos sospechosos comúnmente asociados con la explotación OLE, como los archivos '.rtf'. La implementación de estos mecanismos de detección puede ayudar en la identificación temprana y la respuesta a posibles ataques.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS

- **Balaji, N (2025).** *PoC Exploit Released For Critical Microsoft Outlook (CVE-2025-21298) Zero-Click RCE Vulnerability.* *https://cybersecuritynews.com/outlook-zero-click-rce-vulnerability-cve-2025-21298/*
- **CVE (2025).** *CVE-2025-21298.* https://www.cve.org/CVERecord?id=CVE-2025-21298
- **CVE (2025).** *Required CVE Record Information.* https://www.cve.org/CVERecord?id=CVE-2025-21298
- **GITHUB (2025**). *ynwarcs/CVE-2025-21298.* https://github.com/ynwarcs/CVE-2025-21298/tree/main/diff
- **Jingjing Wu (2025).** *CVE-2025-21298 : Is this CVE applicable for windows server? Is this CRitical and what is resolution ?. . https://answers.microsoft.com/en-us/windowserver/forum/all/cve-2025-21298/784e7214-c083-4e39-8b12-421490fc5eae*
- **MICROSOFT MSCR (2025).** *Windows OLE Remote Code Execution Vulnerability.* https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298
- **OffSec (2025).** *CVE-2025-21298: A Critical Windows OLE Zero-Click Vulnerability. https://www.offsec.com/blog/cve-2025-21298/*