Boletín de alerta

Boletín Nro.:
Fecha de publicación: 10/12/2025
Tema: Alerta 2025-102 Múltiples Vulnerabilidades Identificadas en Productos Windows
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Windows (Kernel, Win32k, Cloud Files Mini Filter, ReFS, Hyper-V, Instalador, PowerShell)**
- **Microsoft Office (Word, Excel, Outlook, SharePoint, LTSC, Mac)**
- **Azure Monitor Agent**
- **Windows Defender Firewall**
- **Microsoft Edge (iOS y Chromium)**
- **Servicios de Aplicaciones, RRAS, Remote Access, DirectX**
- **GitHub Copilot para JetBrains**
- **Componentes de almacenamiento, sistema de archivos y drivers de Windows**

Descripción

Microsoft cerró diciembre de 2025 con la publicación de **56 nuevas actualizaciones de seguridad** diseñadas para corregir fallas críticas en sus sistemas. Estos parches abordan problemas graves, como la capacidad de un atacante para tomar el control total de un equipo (ejecución remota de código), obtener permisos superiores (escalada de privilegios) o exponer datos sensibles. De estas 56 correcciones, **tres son de atención inmediata**: una **vulnerabilidad de «Día Cero»** (que ya está siendo explotada activamente) y dos fallas que habían sido reveladas públicamente. La más crítica es **CVE-2025-62221**, la falla de Día Cero, que permite a un atacante obtener permisos de **SISTEMA** y ha sido catalogada por CISA como de «Explotación Conocida» (KEV), lo que exige su aplicación urgente en todas las organizaciones para evitar un compromiso total del dominio

CVE-2025-62221 – Elevación de Privilegios (Windows Cloud Files Mini Filter)
Esta vulnerabilidad, explotada activamente como día cero, permite que un atacante con acceso limitado al sistema eleve privilegios hasta SYSTEM mediante la manipulación del componente Windows Cloud Files Mini Filter, utilizado por servicios como OneDrive, Google Drive e iCloud; debido al riesgo de que se utilice para comprometer dominios completos, CISA exige su corrección inmediata.

CVE-2025-62554 / CVE-2025-62557 – Ejecución Remota de Código (Microsoft Office)
Estas fallas críticas permiten la ejecución remota de código incluso desde el panel de vista previa sin

necesidad de abrir archivos maliciosos, afectando aplicaciones como Word, Excel, Outlook y versiones LTSC y Mac, lo que facilita ataques altamente efectivos con mínima interacción del usuario.

CVE-2025-64671 – RCE en GitHub Copilot para JetBrains (IDEsaster)
Una vulnerabilidad en la integración de GitHub Copilot con JetBrains permite la ejecución de comandos si un atacante logra manipular la comunicación entre el IDE y el agente MCP, abriendo la puerta a compromisos remotos con solo interferir en el canal de comunicación.

CVE-2025-54100 – RCE en Windows PowerShell (Invoke-WebRequest)
Esta falla permite que un actor no autenticado ejecute código mediante contenido especialmente diseñado que explota la función Invoke-WebRequest de PowerShell, demostrando un comportamiento similar a vulnerabilidades reveladas en investigaciones de seguridad avanzadas.

CVE-2025-62458 – Elevación de Privilegios en Win32k
Una vulnerabilidad en el componente Win32k permite a un atacante escalar privilegios hasta nivel de sistema, representando un riesgo elevado debido a su alta probabilidad de explotación y su potencial para comprometer completamente equipos vulnerables.

CVE-2025-54100 (CVSS 7.8) – Vulnerabilidad de Ejecución Remota de Código en PowerShell
Una neutralización incorrecta de caracteres especiales utilizados en comandos de Windows PowerShell permite que un atacante no autenticado ejecute código de manera local, aprovechando una inyección de comandos. Esta falla representa un riesgo significativo para sistemas donde PowerShell se utiliza en tareas automatizadas o integraciones críticas.

CVE-2025-62562-Microsoft Outlook Vulnerability

Es una vulnerabilidad de uso posterior a la liberación en Microsoft Outlook que permite a un atacante no autenticado ejecutar código de forma remota sin interacción significativa del usuario. Clasificada con un CVSS de 7.8, representa un riesgo importante al posibilitar la ejecución arbitraria de código mediante contenido malicioso.

Solución:

Instalar la actualización de seguridad correspondiente. En la **página de Microsoft** se informa de los distintos métodos para llevar a cabo dichas actualizaciones.

Información adicional:

December 2025 Security Updates – Release Notes – Security Update Guide – Microsoft

Actualizaciones de seguridad de Microsoft de diciembre de 2025 | INCIBE-CERT | INCIBE