BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-05
Fecha de publicación: 15/01/2025
Tema: Múltiples vulnerabilidades críticas en Windows
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Múltiples productos de Microsoft
  - Microsoft Office Excel
  - Active Directory Domain Services
  - Microsoft Office Outlook for Mac
  - Windows BitLocker
  - Windows NTLM
  - Entre otros

Descripción

Recientemente, **Microsoft** publicó un total de 159 vulnerabilidades, incluidas 8 consideradas **Zero-Days**, con tres explotadas activamente en ataques. Estas vulnerabilidades afectan a varios productos como Microsoft Office Excel, Outlook for Mac, Active Directory Domain Services y Windows BitLocker.

De las vulnerabilidades publicadas por Microsoft en su parche mensual de los martes (**Microsoft January 2025 Patch Tuesday**), 12 fueron clasificadas como críticas, incluida la divulgación de información, elevación de privilegios y fallas de ejecución remota de código (RCE).

A continuación, se detallan algunas de las vulnerabilidades más relevantes:

- **CVE-2025-21333, CVE-2025-21334, CVE-2025-21335** – Con un score **CVSS de 7.8**, estas vulnerabilidades **Zero-Day** han sido activamente explotadas para la elevación de privilegios en Windows Hyper-V. Afectan al componente NT Kernel Integration VSP de Microsoft Windows Hyper-V, permitiendo a atacantes locales escalar privilegios a SYSTEM mediante desbordamientos de búfer y errores de uso después de liberación (Use After Free*).

- CVE-2025-21361 – Con una puntuación CVSS de 7.8, esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario en el sistema de destino con los privilegios del usuario que ejecuta Microsoft Outlook asociada con la restricción incorrecta de nombres para archivos y otros recursos. Esto podría dar lugar a un acceso no autorizado a información confidencial, modificación de datos o interrupción de servicios.

- CVE-2025-21294 – Esta vulnerabilidad (CVSS 8.1) permite la ejecución remota de código en la autenticación de Microsoft Digest. Un atacante podría potencialmente obtener el control total del sistema afectado, acceder a información confidencial, modificar datos o interrumpir las operaciones normales. El vector de ataque está basado en la red y no se requiere interacción del usuario, lo que lo hace particularmente peligroso.

- CVE-2025-21362 – Esta vulnerabilidad (CVSS 8.4) está asociada con un problema de uso después de la liberación (Use After Free). El vector de ataque es local y no requiere interacción del usuario ni privilegios para ejecutarse. Esta vulnerabilidad permite a un atacante ejecutar código arbitrario en el sistema de destino a través de Microsoft Excel.

Puedes consultar la lista completa de CVE publicada por Microsoft en el siguiente enlace: Security Update Guide - Microsoft Security Response Center

Recomendamos aplicar las actualizaciones correspondientes para mitigar los riesgos asociados a estas vulnerabilidades lo más pronto posible, especialmente aquellas que están siendo explotadas activamente.

Solución

Es fundamental que los administradores de sistemas y usuarios finales apliquen estas actualizaciones de seguridad lo antes posible para proteger sus sistemas contra posibles explotaciones. Para obtener más detalles y acceder a las actualizaciones, visite el Centro de actualizaciones de seguridad de Microsoft.

Información adicional:

- Microsoft January 2025 Security Updates - Microsoft Community
- CERT-EU - Multiple Vulnerabilities in Microsoft Products
- El martes de parches de enero de 2025 de Microsoft corrige 8 días cero y 159 fallos
- https://encyclopedia.kaspersky.com/glossary/use-after-free/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com