BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-39
Fecha de publicación: 13/05/2025
Tema: Vulnerabilidades Zero-Day en productos Microsoft
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Microsoft Windows 11

Descripción

Se han reportado varias vulnerabilidades críticas Zero Day en productos Microsoft, de las cuales podemos destacar: CVE-2025-30400 con CVSS 7.8, CVE-2025-32701 & CVE-2025-32706 con CVSS 7.8 cada uno, CVE-2025-32709 con CVSS 7.8 y CVE-2025-30397 (tipo RCE) con CVSS 7.5.

A continuación el detalle de las mismas:

1. CVE-2025-30400 (CVSS 7.8) Afecta a la librería Microsoft DWM Core: La cual se explota para obtener privilegios de SISTEMA. El Use after free en Windows, DWM permite a un atacante autorizado elevar los privilegios localmente.

2. CVE-2025-32709 (CVSS 7.8) – Es una escalación de privilegios explotando el controlador de funciones auxiliares de Windows para WinSock. Permite a los atacantes escalar privilegios a Administrador.

3. CVE-2025-30397 (CVSS 7.5) – Una corrupción de memoria que afecta al motor de scripting de Microsoft. Ejecución remota de código activada mediante una URL especialmente diseñada; requiere la interacción del usuario. Este ataque requiere que un usuario autenticado haga clic en un enlace para que un atacante no autenticado pueda iniciar la ejecución remota de código (RCE).

Microsoft reporta que estas 3 vulnerabilidades estan siendo explotadas activamente.

4. CVE-2025-32702 (CVSS 7.8) - Es un RCE para Visual Studio mediante inyección de comandos: Se ejecuta localmente pero se denomina remoto debido a la ubicación del atacante.

5. CVE-2025-26685 (CVSS 6.5) – Afecta al Microsoft Defender con un Identity Spoofing: Permite la suplantación de identidad en redes adyacentes debido a una autenticación incorrecta. La autenticación incorrecta en Microsoft Defender for Identity permite a un atacante no autorizado realizar suplantación de identidad en una red adyacente.
6. CVE-2025-32701 : Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows. El uso posterior a la liberación en el controlador del sistema de archivos de registro común de Windows permite que un atacante autorizado eleve privilegios localmente.

Puede encontrar la lista completa de vulnerabilidades reportadas y abordadas por Microsoft en el siguiente enlace de terceros aquí.

Además, se han reportado varias vulnerabiliadades críticas que afectan a la nube Azure de Microsoft. CVE-2025-29813, CVE-2025-29972, CVE-2025-29827 y CVE-2025-47733. Todas altamente críticas.

- CVE-2025-29813 (con score CVSSv3 10): Vulnerabilidad de elevación de privilegios en Azure DevOps. Microsoft confirmó que esta vulnerabilidad de secuestro de tokens de canalización de Azure DevOps se debe a un problema en el que Visual Studio gestiona incorrectamente los tokens de trabajo de la canalización, lo que permite a un atacante ampliar su acceso a un proyecto. Para explotar esta vulnerabilidad un atacante primero tendría que tener acceso al proyecto e intercambiar el token de corto plazo por uno de largo plazo.
- CVE-2025-29972 (con score CVSSv3 9.9): Vulnerabilidad de suplantación de identidad del proveedor de recursos de almacenamiento de Azure. Microsoft afirmó que esta vulnerabilidad de falsificación de solicitudes del lado del servidor de Azure podría permitir a un atacante autorizado realizar suplantación de identidad (spoofing) en una red.
- CVE-2025-29827 (con score CVSSv3 9.9): Vulnerabilidad de elevación de privilegios en Azure Automation.
- CVE-2025-47733 (con score CVSSv3 9.1): Vulnerabilidad de divulgación de información en Microsoft Power Apps

Solución

En su boletín mensual de seguridad Microsoft (**Microsoft May 2025 Patch Tuesday**) se han liberado parches de seguridad que abordan estas y otras vulnerabilidades puede dirigirse a los siguientes enlaces:

- https://support.microsoft.com/en-us/topic/may-13-2025-kb5058411-os-build-26100-4061-356568c2-c730-469e-819d-b680d43b1265
- https://support.microsoft.com/en-us/topic/may-13-2025-kb5058405-os-builds-22621-5335-and-22631-5335-aa3c8a36-80c4-4c57-91b1-c57b27f3aedb

Las vulnerabilidades en la nube de Microsoft Azure ya han sido mitigadas por el proveedor.

Información adicional:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2025-patch-tuesday-fixes-5-exploited-zero-days-72-flaws/
- https://securityonline.info/microsoft-may-2025-patch-tuesday-fixes-83-vulnerabilities-including-5-exploited-in-the-wild/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.us

contact@cybolt.com

cybolt.com