BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-23
Fecha de publicación: 28/08/2024
Tema: PoC publico que afecta una vulnerabilidad crítica en Windows
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Windows 10 y 11
- Windows Server del 2008 al 2022

Descripción

El 13 de agosto del 2024, se publicó una vulnerabilidad critica identificada como CVE-2024–38063 con una puntuación de 9.8, la vulnerabilidad es de ejecución de código remoto (RCE) en el stack TCP/IP de Windows, que afecta especialmente el protocolo IPv6.

Esta falla Zero-Click (es decir, sin necesidad de intervención del usuario o víctima), permite a los atacantes ejecutar código arbitrario de forma remota a través de paquetes IPv6 especialmente diseñados, lo que puede provocar un compromiso total del sistema. Afecta a los sistemas Windows 10, Windows 11 y Windows Server. Microsoft ha publicado parches para mitigar esta vulnerabilidad y es esencial aplicar estas actualizaciones rápidamente para protegerse contra la explotación.

Un investigador chino de la firma Cyber KunLun descubrió la vulnerabilidad y Microsoft la divulgó públicamente en su lanzamiento del martes de parches de agosto de 2024. Debido a la simplicidad con la que se puede crear un exploit, Microsoft ha instado a los usuarios a aplicar los parches disponibles de inmediato. Algunos expertos en seguridad han aconsejado incorrectamente deshabilitar IPv6. Si bien Microsoft aclara que deshabilitar IPv6 puede mitigar la vulnerabilidad, no se recomienda debido a posibles problemas con la funcionalidad de Windows. En cambio, Microsoft recomienda aplicar parches a los sistemas de inmediato. BeaconLab ya había alertado sobre esta vulnerabilidad en su boletín N° 21 con fecha 21/08/24, sobre Vulnerabilidades Críticas en Windows.

Actualmente, se ha publicado un PoC (Prueba de Concepto) de esta vulnerabilidad, el investigador señala que la versión actual del PoC desencadena una denegación de servicio (DoS) en lugar de una ejecución remota completa del código.
A pesar de esto, la existencia de la PoC sirve como un claro recordatorio del potencial de una mayor explotación, en particular a medida que los atacantes perfeccionan sus técnicas.

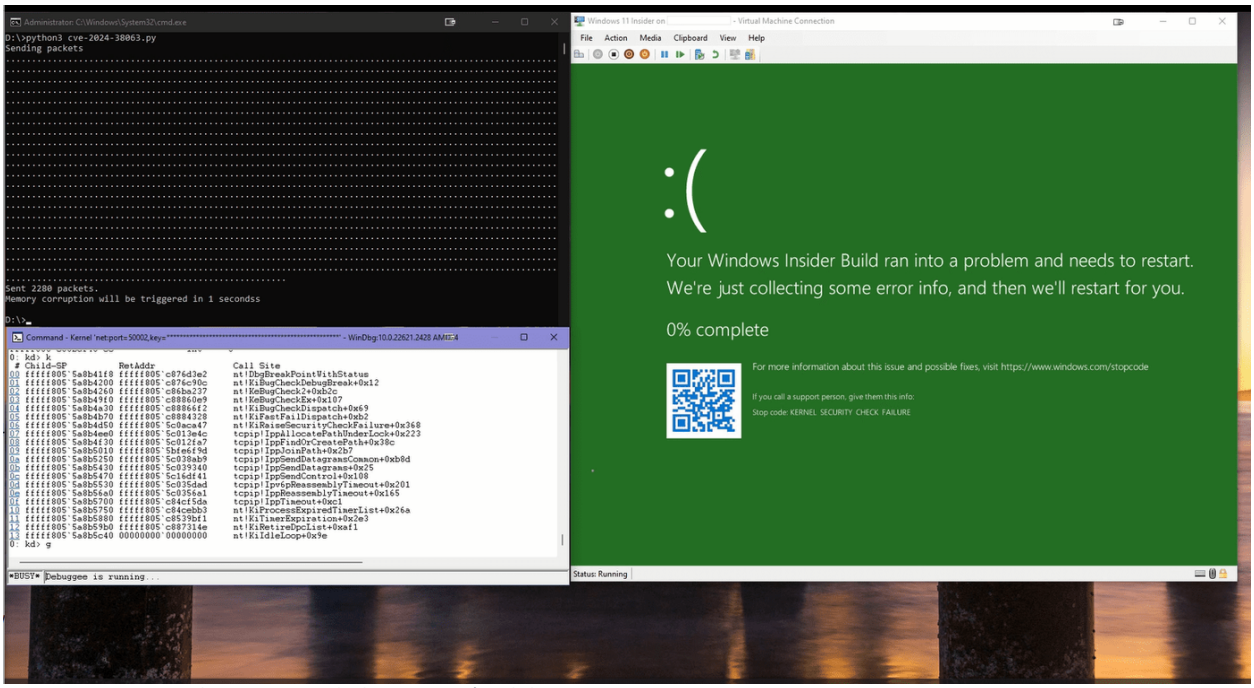

Figura 1 Imagen de muestra de la ejecución del PoC

Actualmente se reportan aproximadamente más 50,000 dispositivos expuestos que podrían estar en riesgo en México, junto con un número indeterminado de computadoras que operan con Windows 10 y Windows 11.

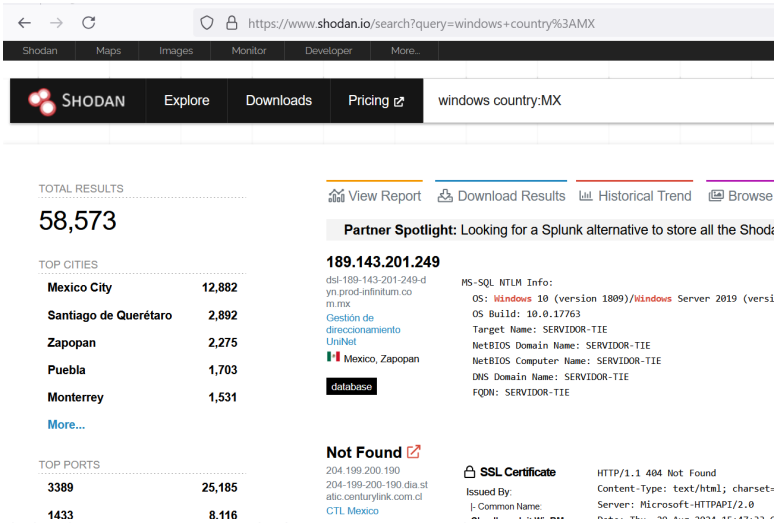

Figura 2 Cantidad de dispositivos con algún Sistema Windows expuesto a Internet. Imagen extraída de Shodan.

Solución

Microsoft ha lanzado una actualización de seguridad para abordar esta vulnerabilidad. Se recomienda encarecidamente instalar esta actualización lo antes posible. Puede encontrar la actualización y más información en el Centro de Respuesta de Seguridad de Microsoft:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063?ref=thestack.technology

Actualización para Windows 11:

- https://support.microsoft.com/en-us/topic/august-13-2024-kb5041571-os-build-26100-1457-d218c08d-8de2-4f9a-8fe1-a2c2fd83ca9a

Actualización para Windows 10:

- https://support.microsoft.com/en-us/topic/august-13-2024-kb5041580-os-builds-19044-4780-and-19045-4780-2ef55b0d-bb01-41c8-8629-4146929792ad

Actualización para Windows 2012:

- https://support.microsoft.com/en-us/topic/august-13-2024-kb5041828-monthly-rollup-7e0dccac-5746-4cac-b413-8f9182a625d0

Si no puede instalar la actualización de inmediato, puede mitigar el riesgo deshabilitando IPv6 en sus sistemas vulnerables. Sin embargo, esto puede afectar la conectividad y la funcionalidad de la red.

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063?ref=thestack.technology
- https://www.rapid7.com/db/vulnerabilities/msft-cve-2024-38063/
- https://securityonline.info/zero-click-windows-rce-threat-researcher-publishes-poc-exploit-for-cve-2024-38063/
- https://beaconlab.mx/publicacion/multiples-vulnerabilidades-criticas-en-windows/
- https://www.cve.org/CVERecord?id=CVE-2024-38063

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com