BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-34
Fecha de publicación: 17/09/2024
Tema: POC Público para CVE-2024-38080 en Hyper-V
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Windows Hyper-V

Descripción

En julio se había publicado la vulnerabilidad CVE-2024-38080 (CVSS 7.8) la cual afecta a Windows Hyper-V, el hipervisor de Microsoft utilizado para entornos virtualizados. Se trata de una vulnerabilidad de elevación de privilegios (EoP) que ya ha sido explotada en la naturaleza y está incluida en el Catálogo de Vulnerabilidades Explotadas Conocidas de CISA.

El fallo reside en la función VidExoBrokerIoctlReceive de Hyper-V y proviene de un desbordamiento de enteros, lo que permite a actores malintencionados manipular la memoria del sistema. Al explotar esta vulnerabilidad, los atacantes pueden ejecutar código con privilegios a nivel de SYSTEM, logrando el control total del sistema comprometido.

Recientemente, un investigador de seguridad publicó un análisis detallado y un código de prueba de concepto (PoC) para esta vulnerabilidad crítica, que ya ha sido parcheada en Windows Hyper-V, dicha vulnerabilidad representa un riesgo significativo para las organizaciones que dependen de la virtualización de Microsoft.

El PoC de esta vulnerabilidad está disponible públicamente en GitHub, lo que incrementa el riesgo para las organizaciones que utilizan Hyper-V para cargas de trabajo críticas, ya que proporciona una guía clara para que los atacantes puedan replicar el exploit, por lo que es probable que empiece a explotarse activamente en el corto tiempo.

Solución

Microsoft ha lanzado un parche que aborda esta vulnerabilidad. Dirígete al sitio oficial de Microsoft o a Windows Update para aplicar la actualización de seguridad correspondiente a esta vulnerabilidad. Asegúrate de que todos los servidores y entornos Hyper-V estén completamente actualizados.
https://msrc.microsoft.com/update-guide/releaseNote/2024-Jul

Información adicional:

- https://msrc.microsoft.com/update-guide/releaseNote/2024-Jul
- GitHub - pwndorei/CVE-2024-38080: poc code for CVE-2024-38080
- [Investigación] Clase de 1 día de Hyper-V: CVE-2024-38080 - hackyboiz
- Nicolas Krassas en X: "Exploit PoC lanzado para la vulnerabilidad de día cero de Windows Hyper-V CVE-2024-38080 https://t.co/q7NxMSbyXx" / X

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com