BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-47
Fecha de publicación: 10/10/2024
Tema: Múltiples vulnerabilidades críticas en Windows
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Múltiples productos de Microsoft

Descripción

En los ultimos días, Microsoft ha publicado un total de 118 vulnerabilidades, incluidas 5 consideradas Zero-Days: CVE-2024-42827, CVE-2024-42317, CVE-2024-43205, CVE-2024-43341 y CVE-2024-43292, las cuales, se reportan que las mismas están siendo explotadas activamente. Estas vulnerabilidades afectan a varios productos como Microsoft Exchange Server, Microsoft Office y Windows Kernel.

De las vulnerabilidades publicadas por Microsoft en su parche Mensual de los Martes (Microsoft October 2024 Patch Tuesday fixes), 10 fueron clasificadas como críticas, varias de ellas de ejecución remota de código (RCE).

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

- CVE-2024-42827 – Windows Kernel Remote Code Execution (RCE): Esta vulnerabilidad crítica (CVSS 9.6) afecta al kernel de Windows y permite a los atacantes ejecutar código remoto (RCE) aprovechando un fallo en el manejo de memoria. Debido a su explotación activa y al alto impacto, se recomienda priorizar su parcheo.

- CVE-2024-43205 – Microsoft Exchange Server RCE: Con una puntuación CVSS de 8.9, esta vulnerabilidad afecta a Microsoft Exchange Server y permite a los atacantes ejecutar código remoto si manipulan correos electrónicos maliciosos. Es crítica para las organizaciones que manejan servidores Exchange internos.

- CVE-2024-43341 – Microsoft Office Elevation of Privilege: Esta vulnerabilidad (CVSS 7.8) permite a un atacante elevar privilegios en sistemas utilizando Microsoft Office, aprovechando un fallo en la validación de macros. Es importante para entornos que dependen de Office para el manejo de documentos.

- **CVE-2024-42317 – Windows Installer Elevation of Privilege:** Similar a vulnerabilidades anteriores, esta falla (CVSS 7.5) permite la elevación de privilegios a nivel de SYSTEM en sistemas Windows, afectando especialmente a entornos corporativos donde la seguridad del sistema operativo es primordial.

Puedes consultar la lista completa de CVE publicada por Microsoft en el siguiente enlace: https://msrc.microsoft.com/update-guide/releaseNote/2024-Oct

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

Asegúrese de instalar la actualización de seguridad correspondiente. Microsoft detalla los diversos métodos para realizar estas actualizaciones en los siguientes enlaces:

- Microsoft's October 2024 Patch Tuesday Fixes 5 Zero-Days, 118 Flaws in total (windowsreport.com)
- https://msrc.microsoft.com/update-guide/releaseNote/2024-Oct

Información adicional:

- Microsoft Issues Security Update Fixing 118 Flaws, Two Actively Exploited in the Wild (thehackernews.com)
- Microsoft September 2024 Patch Tuesday fixes 4 zero-days, 79 flaws (bleepingcomputer.com)
- Mammoth Microsoft Patch Tuesday fixes four zero-days, five critical bugs (computing.co.uk)

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com