BEACON LAB
C S I R T

CYBOLT

Boletín de alerta

Boletín Nro.: 2024-67
Fecha de publicación: 11/12/2024
Tema: Alerta 2024-67 Vulnerabilidades criticas RCE en productos Microsoft
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Múltiples productos de Microsoft**
  - Aplicaciones y servicios de Microsoft Office
  - Seguridad del sistema y gestión de endpoints
  - Componentes y servicios de Windows
  - Servicios de autenticación y red
  - Infraestructura y roles de servidor
  - Otros componentes críticos

Descripción

Se ha reportado la explotación activa de un vulnerabilidad de Día Cero (Zero-Day) etiquetada como CVE-2024-49138 con un score de CVSSv3 de 7.8 que afecta al controlador del sistema de archivos de registro común (CLFS) de Windows, que permite elevación de privilegios. Aunque los detalles sobre su explotación aún no son públicos, esta vulnerabilidad representa un riesgo significativo para los sistemas afectados.

Además se publicaron varias vulnerabilidades importantes y criticas como:

- **CVE-2024-49118, CVE-2024-49122:** Son vulnerabilidades de tipo ejecución remota de código RCE que afectan al Microsoft Message Queuing (MSMQ). A ambas se les asignó una puntuación CVSSv3 de 8,1 y se las considera críticas. Según Microsoft, para que se aprovechen con éxito, es necesario que un atacante supere una condición de carrera. Para que un sistema sea vulnerable, se debe agregar y habilitar el servicio MSMQ. Si el servicio está habilitado en una instalación de Windows, se ejecutará un servicio llamado «Message Queueing» en el puerto TCP 1801.

- **CVE-2024-49106, CVE-2024-49108, CVE-2024-49115, CVE-2024-49116, CVE-2024-49119, CVE-2024-49120, CVE-2024-49123, CVE-2024-49128 and CVE-2024-49132:** son vulnerabilidades de ejecución remota de commandos (RCE) que afectan a los Servicios de Escritorio remoto (RDP) de Windows. Todas las vulnerabilidades recibieron una puntuación CVSSv3 de 8.1. La explotación requiere que un atacante active una condición de carrera (race condition) para «crear un escenario de uso después

de la liberación» (create a use-after-free scenario) que podría conducir a la ejecución de código arbitrario.

El equipo de Microsoft ha publicado en su publicación de actualizaciónes de diciembre 2024 los parches de seguridad que abordan estas vulnerabilidades. Para ver la lista de todas las vulnerabilidades afectadas puede encontrar **aquí**

Solución

Es fundamental que los administradores de sistemas y usuarios finales apliquen las actualizaciones de seguridad propuesta por el proveedor lo antes posible.

Para obtener más detalles y acceder a las actualizaciones, visite el siguiente enlace:

https://msrc.microsoft.com/update-guide/releaseNote/2024-Dec

Información adicional:

- **https://msrc.microsoft.com/update-guide/releaseNote/2024-Dec**
- **https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2024-patch-tuesday-fixes-1-exploited-zero-day-71-flaws/?&web_view=true**
- **https://www.tenable.com/blog/microsofts-december-2024-patch-tuesday-addresses-70-cves-cve-2024-49138**