ALERTA

Ataques de Ejecución Remota de Código en Windows

COLCERT AL-1207-034

TLP:CLEAR

” Por medio de Archivos .url se pueden infectar dispositivos”

Actores maliciosos están utilizando una nueva técnica para explotar una vulnerabilidad de ejecución remota de código (RCE) en sistemas Windows. Los ataques aprovechan archivos de acceso directo de Internet (.url) especialmente diseñados para abrir el navegador Internet Explorer (IE) descontinuado y ejecutar código malicioso en la computadora de la víctima, incluso en sistemas Windows 10 y 11 completamente parcheados.

RCP/RCE

Impacto en la seguridad digital:

Los ataques exitosos pueden permitir a los atacantes ejecutar código arbitrario en la computadora de la víctima, lo que podría conducir al robo de datos, la instalación de malware o el control total del sistema.

Vector de ataque: “.url que contienen el esquema "ms-dtc”

Sistemas afectados y detalles:

Sistemas operativos: Windows
Navegadores web: Internet Explorer
Vulnerabilidad: Los ataques explotan una vulnerabilidad en la forma en que Windows maneja los archivos .url que contienen el esquema "ms-dtc"

Para protegerse y evitar técnicas de estos ciberataques:

Los ataques utilizan el truco "mhtml" para eludir la configuración predeterminada del navegador y abrir IE, y ocultan la extensión .hta maliciosa para disfrazar el archivo como un PDF.

Aplicar el parche de seguridad: Instalar la actualización de seguridad de Microsoft (CVE-2024-38112)

Mantenerse informado: Seguir las alertas de seguridad de Microsoft y otras fuentes confiables para estar al tanto de las últimas amenazas y vulnerabilidades.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://research.checkpoint.com/2024/resurrecting-internet-explorer-threat-actors-using-zero-day-tricks-in-internet-shortcut-file-to-lure-victims-cve-2024-38112/
https://www.scmagazine.com/news/internet-explorer-still-used-as-a-malware-vehicle-by-threat-actors
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

COLCERT