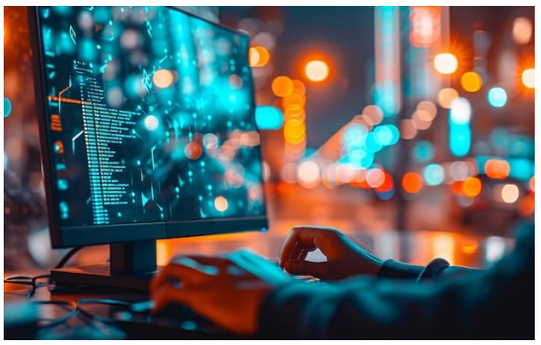
ALERTA

TEMA DE ANÁLISIS: Explotación de RCE en Protocolo TCP/IP de Windows

[COLCERT AL-2008-039]

TPL: CLEAR

Microsoft advierte sobre la vulnerabilidad CVE-2024-38063. Esta vulnerabilidad ha sido categorizada como crítica y permite la ejecución remota de código (RCE) en sistemas Windows con IPv6 habilitado. La información disponible incluye detalles técnicos sobre la vulnerabilidad, su potencial impacto y recomendaciones de mitigación.



ELEMENTOS DE INTELIGENCIA DISPONIBLES

Pérdida de datos: Los atacantes podrían robar o destruir datos confidenciales.**Disrupción de servicios:** Los sistemas comprometidos podrían ser utilizados para lanzar ataques a otros sistemas o para realizar actividades maliciosas.**Espionaje industrial:** Los atacantes podrían obtener acceso a información sensible de propiedad intelectual.**Extorsión:** Los atacantes podrían cifrar los datos de las víctimas y exigir un rescate para su liberación

ANÁLISIS

La vulnerabilidad CVE-2024-38063 explota una debilidad en el protocolo TCP/IP de Windows, permitiendo a atacantes remotos ejecutar código arbitrario en sistemas vulnerables sin requerir interacción del usuario. La clasificación como "wormable" indica que esta vulnerabilidad podría propagarse de forma autónoma a través de una red, amplificando significativamente el impacto de un ataque exitoso. La naturaleza crítica de esta vulnerabilidad y la facilidad de explotación hacen que sea una amenaza inminente para organizaciones de todos los tamaños.

IMPACTO PARA COLOMBIA Y LA REGIÓN

Priorizar la actualización de sistemas: Las organizaciones deben considerar esta vulnerabilidad como una amenaza de alto riesgo **Comunicar la amenaza:** Informar a todos los usuarios de la organización sobre el riesgo y las medidas de mitigación.**Evaluar la exposición y mitigación.**

NIVEL DE RIESGO

MEDIO

FUENTES:

https://securityaffairs.com/167117/hacking/windows-rce-tcp-ip.html
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063
https://securityaffairs.com/167000/security/microsoft-patch-tuesday-august-2024.html
https://isc.sans.edu/diary/rss/31186

COLCERT