Nro. Alerta:	AL-2024-18	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	16-ago-2024	**Vulnerabilidad crítica de ejecución remota que afecta a TCP/IP en sistemas Windows CVE-2024-38063**	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

Microsoft advirtió este martes 13 de agosto a sus clientes, que parchen una vulnerabilidad crítica en la pila TCP/IP de Windows cuando IPv6 está habilitado; la explotación de esta vulnerabilidad permite la ejecución remota de código (RCE) sin la interacción del usuario, lo que la convierte en una vulnerabilidad de "0 clic".

Esta vulnerabilidad de código remoto permite a un atacante no autenticado, enviar repetidamente paquetes IPv6, que incluyen paquetes especialmente diseñados, a una máquina Windows, lo que podría permitir la ejecución remota de código.
Se le ha asignado una puntuación CVSS de 9,8 y el código CVE-2024-38063.

Figura 1: Imagen referencial de la vulnerabilidad *CVE-2024-38063*

III. INTRODUCCIÓN

Microsoft ha publicado una actualización de seguridad urgente para solucionar una vulnerabilidad crítica de ejecución remota de código en la pila TCP/IP de Windows. La falla identificada con el CVE-2024-38063, afecta a todas las versiones compatibles de Windows y Windows Server, incluidas las instalaciones de Server Core.

Un atacante puede explotar esta vulnerabilidad de forma remota enviando paquetes IPv6 especialmente diseñados a un host de destino; no se requiere interacción del usuario, lo que la convierte en una vulnerabilidad de “0 clic”.

Sólo los paquetes IPv6 pueden ser utilizados de forma indebida para explotar esta vulnerabilidad por lo que Microsoft recomienda deshabilitar IPv6 si no es necesario ya que la explotación exitosa de CVE-2024-38063 podría permitir a un atacante ejecutar código arbitrario en el sistema de destino con privilegios SYSTEM. Este nivel de acceso le daría al atacante control total sobre la máquina comprometida.

Dada la naturaleza crítica de esta vulnerabilidad y su potencial impacto generalizado, las organizaciones deben tratar el abordaje de CVE-2024-38063 como una máxima prioridad.

A continuación, opciones de remediación:

- **Remediación inmediata:** Microsoft ha publicado la actualización de seguridad para esta vulnerabilidad en el sitio oficial de Microsoft (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38063); ir a la sección de Security Updates y en la columna Product es posible encontrar la actualización de seguridad correspondiente a cada una de las versiones de sistema operativo tanto como de la arquitectura utilizada como se destaca en la siguiente imagen:

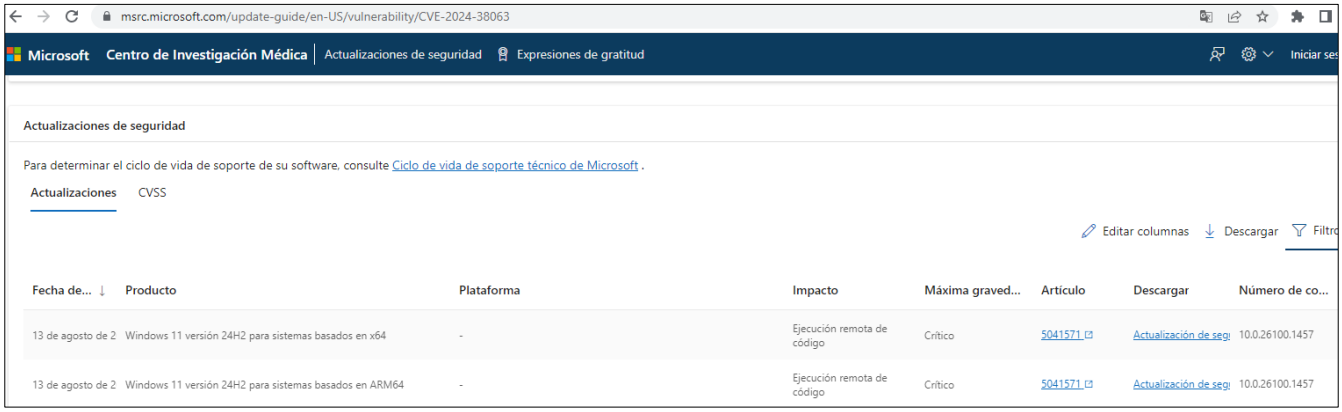

Figura 2: Actualizaciones disponibles en el portal de Microsoft
Fuente: Microsoft

- **Remediación parcial**

Se tiene la posibilidad de poder remediar esta vulnerabilidad inhabilitando IPv6 desde las propiedades de la tarjeta de red de los equipos de usuarios que no requieren:

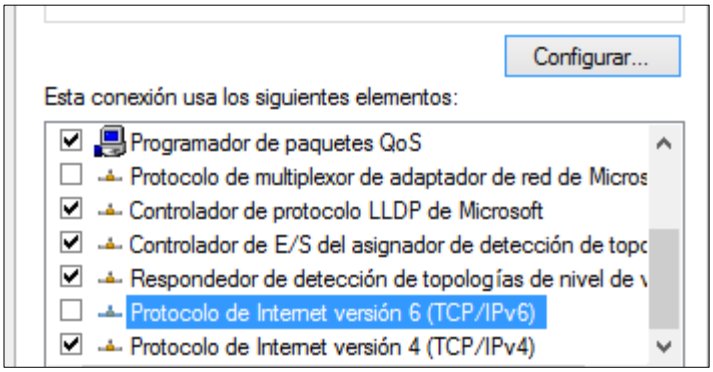

Figura 3: Propiedades de la tarjeta de red para deshabilitar IPv6

Para servidores Windows Server 2008/2012/2016/2019/2022 se tienen tres posibilidades: Haciendo uso del administrador del servidor, haciendo uso de los registros de Windows o mediante powershell haciendo uso de los cmdlets.

Opción 1: Mediante administrador del servidor

- Ir las propiedades del adaptador de red activo
- Desmarcar la casilla ***Protocolo de Internet versión 6 (TCP/IPv6)*** y clic en **Aceptar** para aplicar los cambios.

Opción 2: Mediante registros del Windows (Reinicio de servidor)

- Abra el regedit.
- Dentro de la siguiente dirección: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters***, crear un nuevo valor DWORD (32 bits) llamado **DisableComponents**. Para deshabilitar completamente ipv6 se debe asignar el valor ***0xffffffff*** y Reiniciar el servidor

Opción 3: Utilizando Powershell

- Ejecutar powershell como administrador.
- Ejecutar el siguiente comando para realizar la deshabilitación a UNA interfaz de red: ***Disable-NetAdapterBinding -Name "Ethernet" -ComponentID ms_tcpip6***
- Ejecutar el siguiente comando para realizar la deshabilitación a todas las interfaces de red: ***Get-NetAdapter | Disable-NetAdapterBinding -ComponentID ms_tcpip6***
- Para encontrar los nombres de las interfaces de red es posible obtenerla mediante el siguiente comando en powershell: ***Get-NetAdapter | Select-Object Name***

IV. VECTOR DE ATAQUE:

CVE-2024-38063: es una vulnerabilidad crítica de RCE que afecta a TCP/IP de Windows; Microsoft la clasifica como "Explotación más probable" ya que la complejidad para el atacante es bajo porque no necesita acceder a ninguna configuración o archivo para llevar a cabo el ataque y se podría explotar esta vulnerabilidad de forma remota enviando paquetes IPv6 especialmente diseñados a un host; por lo que, los sistemas no se ven afectados si IPv6 está deshabilitado en la máquina de destino.

V. RECOMENDACIONES:

Los expertos en seguridad recomiendan las siguientes acciones:

- Aplique las últimas actualizaciones de seguridad de Microsoft inmediatamente.
- Priorizar la aplicación de parches en los sistemas conectados a Internet.
- Considerar deshabilitar IPv6 si no es necesario en su entorno de red.
- Monitorear cualquier actividad de red sospechosa, particularmente aquella que involucre tráfico IPv6.
- Implementar la segmentación de la red para limitar el posible movimiento lateral si un sistema se ve comprometido.

VI. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VII. REFERENCIAS:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38063
- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/2022/
- https://www.cve.org/CVERecord?id=CVE-2024-38063
- https://www.cybermaxx.com/resources/cve-2024-38063/
- https://cybersecuritynews.com/0-click-rce-windows-tcp-ip/
- https://www.it-connect.fr/cve-2024-5274-la-8eme-faille-zero-day-de-2024-corrigee-dans-google-chrome/