CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad Windows Point-to-Point Tunneling Protocol

Fecha: 04/01/2023

Problemática: Vulnerabilidades del protocolo Tunneling P to P de Windows

Correlativo: AC-0004

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Microsoft ha emitió un comunicado para informar a sus usuarios sobre las múltiples vulnerabilidades identificadas como CVE-2022-41081, CVE-2022-38000, CVE-2022-38047, CVE-2022-33634, CVE-2022-24504, CVE-2022-22035, CVE-2022-30198 que afectan al protocolo Point-to-Point de Sistemas Operativos Windows.

SITUACIÓN

La explotación exitosa de esta vulnerabilidad requiere que un atacante gane una condición de carrera y para aprovechar esta vulnerabilidad, un atacante necesitaría enviar un paquete PPTP malicioso especialmente diseñado a un servidor PPTP (Point to Point Tunneling Protocol). Esto podría resultar en la ejecución remota de código en el lado del servidor.

Programáticamente, la condición de carrera es el escenario en el que dos o más subprocesos intentan acceder a un recurso compartido, como una variable o un código, y cambiarlo al mismo tiempo debido a una ejecución indeterminada del subproceso en el algoritmo de programación de subprocesos.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alto**

RECOMENDACIONES

- Se recomienda a los usuarios de Sistemas Operativos de Microsoft Windows a realizar la actualización correspondiente de acuerdo a la versión que corresponda.
- Active las funciones de actualización automática de software en computadoras siempre que sea posible y pragmático.
- Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.

DICCIONARIO DE DATOS

- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
- Código arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
- CVE (Common Vulnerabilities and Exposures); Listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad.
- Condición de carrera: situación indeseable que ocurre cuando un dispositivo o sistema intenta realizar dos o más operaciones al mismo tiempo.

REFERENCIAS

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41081
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38000
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38047
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24504
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22035
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30198