

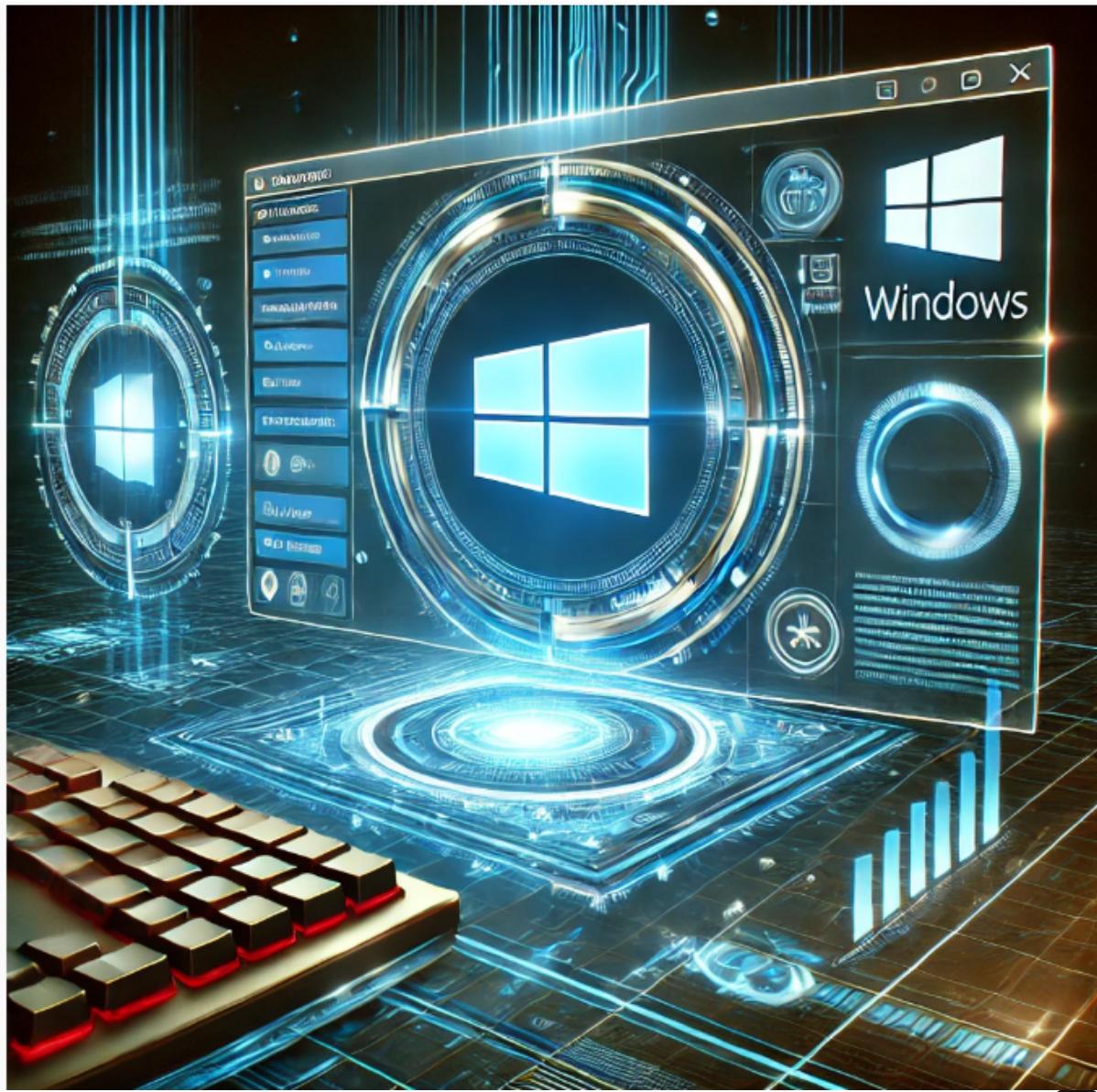
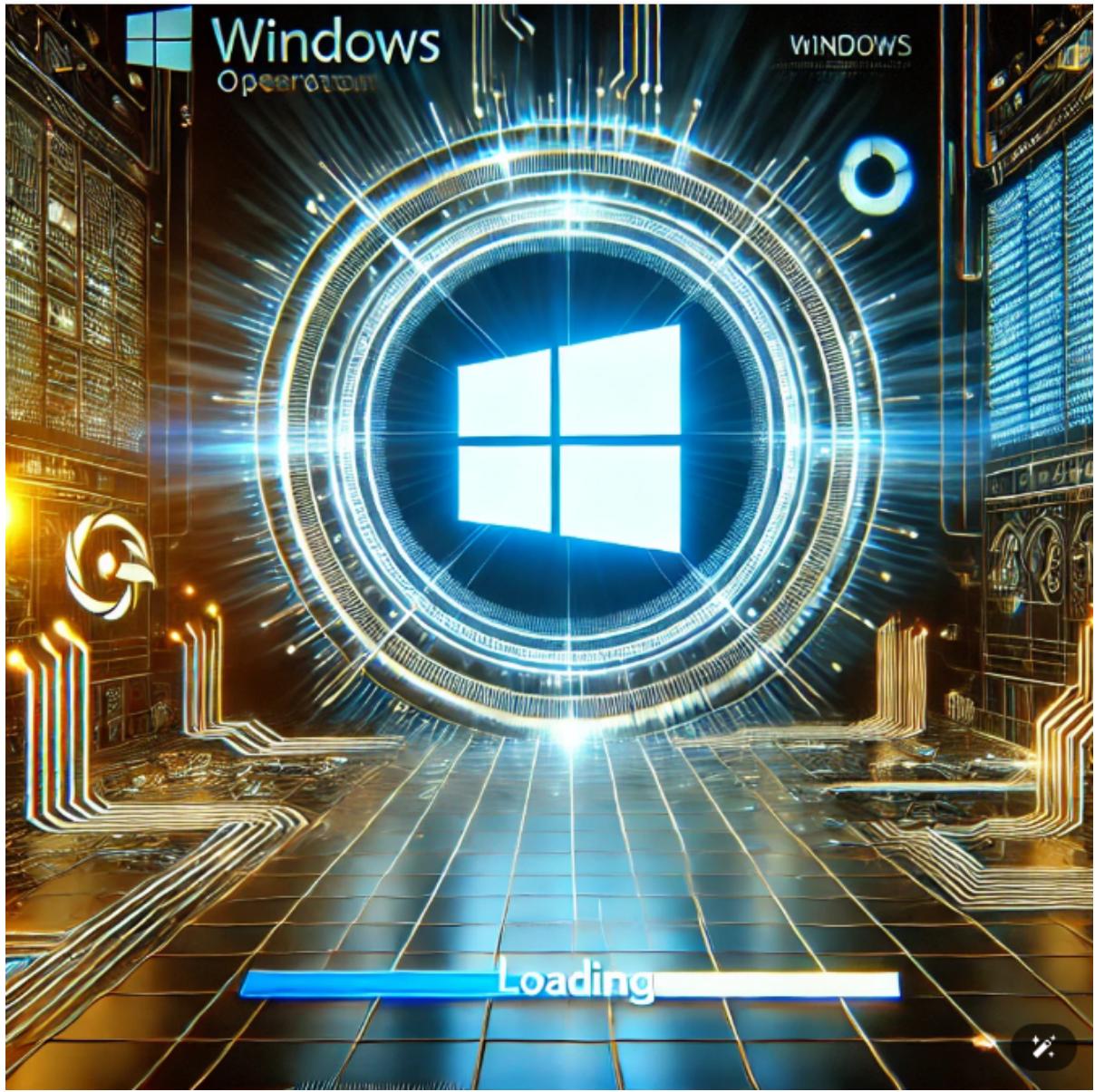
Microsoft Windows Bluetooth Remote Code Execution Vulnerability



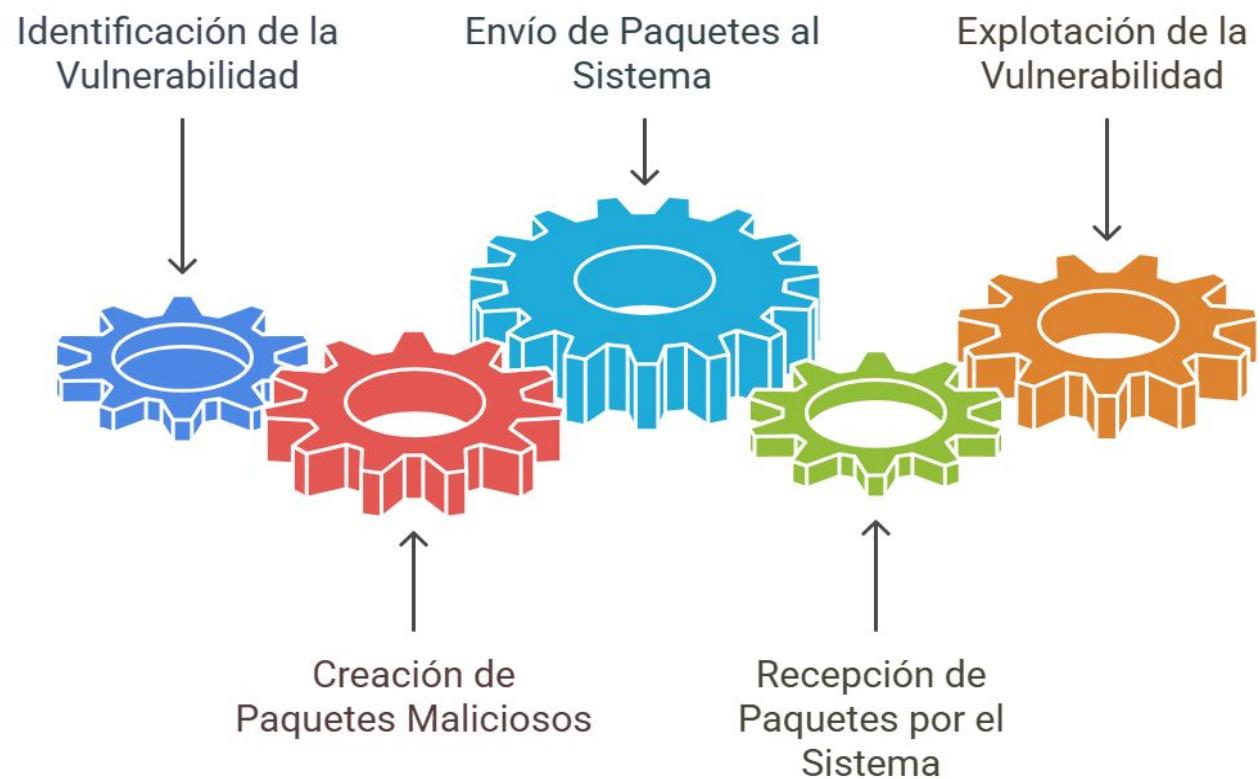
Microsoft Bluetooth

Bluetooth Firk Rietoote
Tecetion Vulenitly

- CC Diego Cabuya
- MY Sergio Cruz
- MY López Victor
- MY Yerson Torres



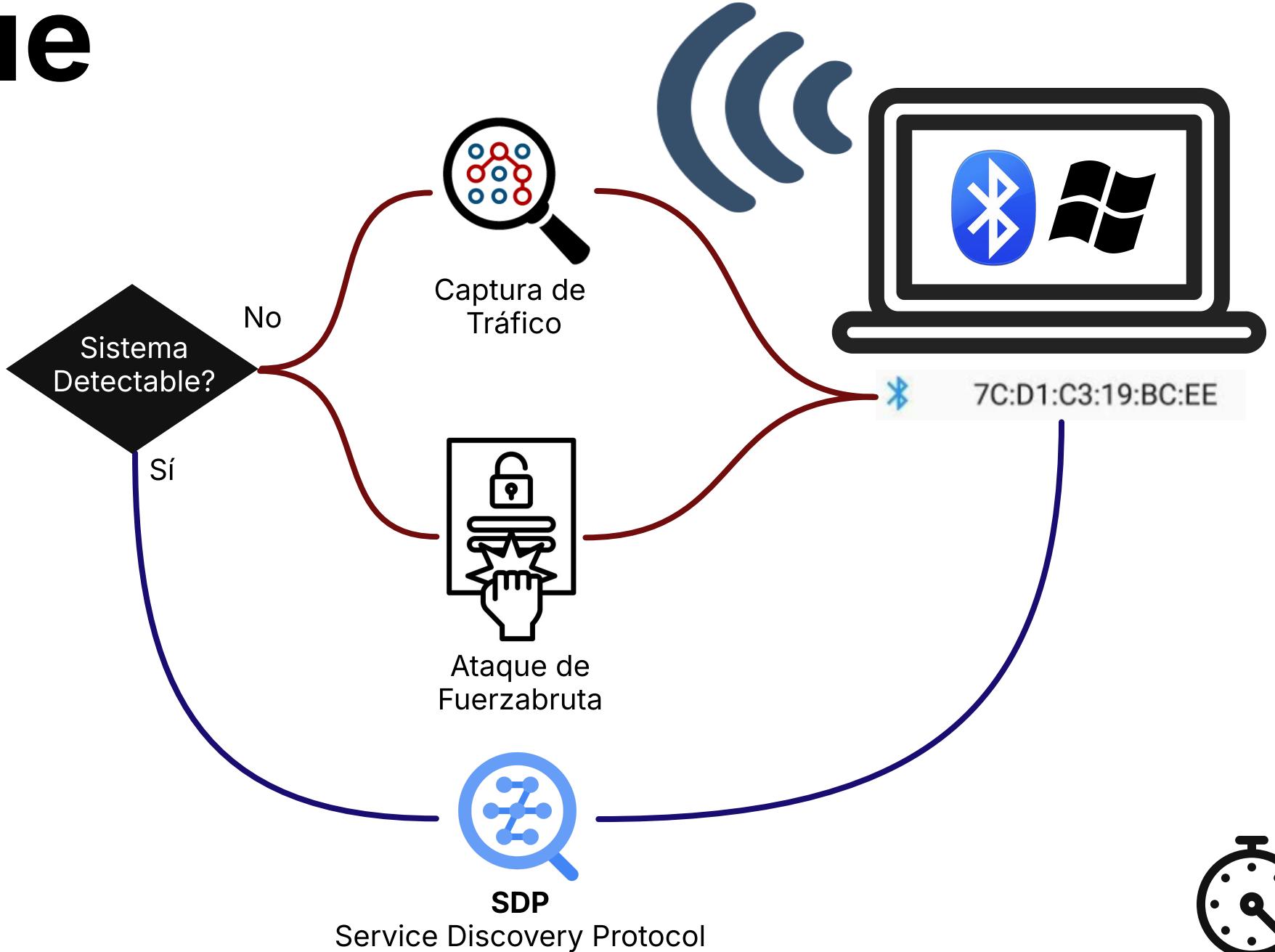
Secuencia de Explotación de Vulnerabilidad de Bluetooth



El Ataque



- Instalar programas
- Ver, cambiar o eliminar datos
- Crear nuevas cuentas



CVSS v3.1

Vector de ataque → Adyacente a la red

- Atacante en proximidad de la maquina.
- Alcance de conectividad depende de la clase y la versión del dispositivo Bluetooth.
- En el mejor de los casos 400 mts.

Complejidad del ataque → Bajo

- El equipo a atacar debe tener la opción de Bluetooth encendida.
- El atacante recibira la dirección del dispositivo.
- Por diseño del protocolo la complejidad es sencilla.

Privilegios requeridos → Ninguno

- Por diseño del protocolo no se requiere ningun privilegio para ejecutar el ataque.

Interacción → Ninguna

- No se requiere ninguna interaccion



CVSS v3.1

Impacto en la Confidencialidad → Alto

Acceder a información clasificada:

- Registros de inspecciones subacuáticas.
- Datos de misiones estratégicas.
- Credenciales de oficiales o usuarios del sistema.

Impacto en la Integridad → Alto

Alterar registros de inspección subacuática :

- Alterar informes de inspección o registros de actividad.
- Ejecutar código malicioso mediante la explotación de memoria.
- Ataques de falsificación de identidad Creación de cuentas

Impacto en la Disponibilidad → Alto

Bloquea el uso del Bluetooth

- Desactivación de sistemas Bluetooth sensores
- Bloqueo de dispositivos
- Destrucción de datos críticos

Análisis del Impacto en el Sistema

