CVE-2011-1265

MICROSOFT WINDOWS BLUETOOTH REMOTE CODE EXECUTION VULERABILITY

GRUPO 5

URIBE CARLOS
MY

DANNY SANCHEZ
CC

JOSE MARTINEZ
CC

Sistema Vulnerable

Microsoft

OS:

Windows Vista SP1 y SP2
Windows 7 Gold y SP1

Servicio Vulnerado:

Bluetooht Stack 2.1

Técnicas de Explotación

- Escaneo de dispositivos Bluetooth (48 bits)
- Proximidad a la maquina objetivo, fin Rx y Tx por LOS
- Envio de Paquetes maliciosos
- Ejecucion de Codigo malicioso (Ver, cambiar o eliminar datos)

CVSS BASE v3.1
SCORE: 8.8

VECTOR DE ATAQUE

RED ADYACENTE
Se necesita que el equipo atacante este en la misma proximidad de la maquina objetivo.

COMPLEJIDAD DEL ATAQUE

BAJA COMPLEJIDAD
Bluetooth activo, obtener la direccion del trafico.

PRIVILEGIOS REQUERIDOS

NINGUNO
Un atacante no necesita privilegios para ejecutar un ataque.

INTERACCION DEL USUARIO

NINGUNO
No se requiere interaccion del usuario para el ataque.

CVSS BASE v3.1
SCORE: 8.8

ALCANCE

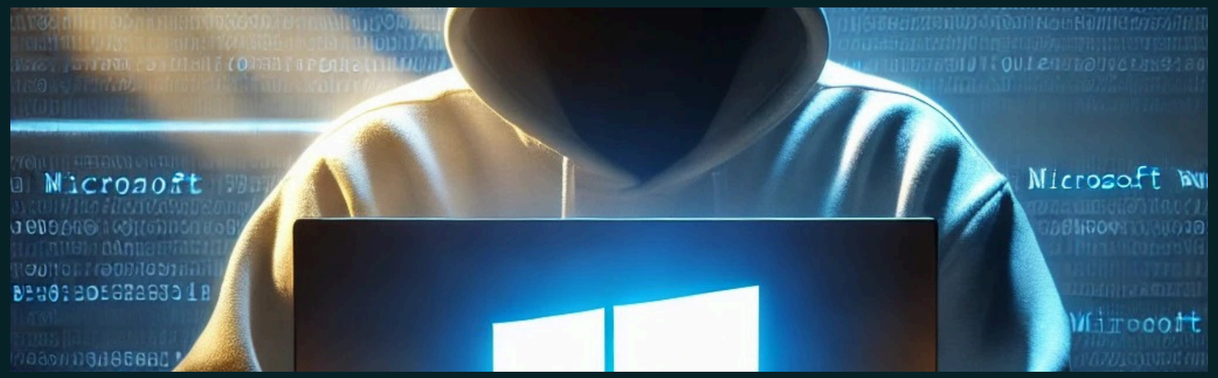
SIN CAMBIOS
El componente vulnerable y el componente afectado son el mismo OS.

CONFIDENCIALIDAD

INTEGRIDAD

ALTO
El atacante puede ver, cambiar o eliminar datos, o crear nuevas cuantas con todos los derechos de usuario.

DISPONIBILIDAD



Medidas de Mitigación

- Aplicar actualizaciones de seguridad.
- Deshabilitar Bluetooth si no es necesario.
- Usar Firewall o restricciones de conexiones bluetooth.
- Actualizar controladores y software de Bluetooth.

THANK YOU

This sentence contains information related to the title