	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 17-03-2023
		Página 18 de 24

Componente que reporta	**CENTRO DE OPERACIONES CIBERESPACIALES**		
Nombre de la alerta	Microsoft lanza actualizaciones para 80 nuevas fallas de seguridad.		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. El día 15 de marzo del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se logró identificar nuevos parches de seguridad de Microsoft, las cuales se están implementando como solución para un conjunto de 80 fallas de seguridad; de las cuales, 8 errores se califican como críticos, 71 como importantes y 1 como moderado en gravedad.

   Cabe resaltar, que dos de las vulnerabilidades han sido atacadas activamente, donde se incluye una falla de escalada de privilegios de Microsoft Outlook (CVE-2023-23397 , puntaje CVSS: 9.8) y una omisión de la función de seguridad de Windows SmartScreen (CVE-2023-24880 , puntaje CVSS: 5.1).

   La vulnerabilidad CVE-2023-23397 se activa cuando un atacante envía un mensaje con una propiedad MAPI extendida con una ruta UNC a un recurso compartido SMB (TCP 445) en un servidor controlado por un actor de amenazas y la vulnerabilidad CVE-2023-24880 se refiere a una falla de omisión de seguridad que podría explotarse para evadir las protecciones Mark-of-the-Web (MotW) al abrir archivos no confiables descargados de Internet.

   Finalmente, se dio a conocer una lista de los productos de Microsoft que constan con las actualizaciones de seguridad, que a continuación se detalla:

   - Azur
   - Subsistema de tiempo de ejecución del servidor del cliente (CSRSS)
   - Protocolo de mensajes de control de Internet (ICMP)
   - Controlador Bluetooth de Microsoft
   - Dinámica de Microsoft
   - Microsoft Edge (basado en cromo)
   - Componente de gráficos de Microsoft
   - Excel de Microsoft Office
   - Microsoft Office Outlook
   - Microsoft Office SharePoint
   - Microsoft onedrive
   - Controlador de impresora Microsoft PostScript
   - Controladores de impresora de Microsoft
   - Biblioteca de códecs de Microsoft Windows
   - Oficina para Android
   - Servicio de acceso remoto Protocolo de tunelización punto a punto
   - Rol: Servidor DNS
   - Rol: Windows Hyper-V
   - Tejido de servicio
   - Estudio visual
   - Control de cuentas de Windows
   - Servicio Bluetooth de Windows
   - Administrador de recursos centrales de Windows
   - Servicios criptográficos de Windows
   - Defensor de Windows
   - Pila de protocolo HTTP de Windows

- Windows HTTP.sys
- Protocolo de intercambio de claves de Internet de Windows (IKE)
- Núcleo de Windows
- Controlador de administración de particiones de Windows
- Protocolo punto a punto de Windows a través de Ethernet (PPPoE)
- Llamada a procedimiento remoto de Windows
- Tiempo de ejecución de llamada a procedimiento remoto de Windows
- Sistema de archivos resistente de Windows (ReFS)
- Canal seguro de Windows
- Pantalla inteligente de Windows
- TPM de Windows
- Windows Win32K

2. Recomendaciones:

- Se recomienda que el personal encargado del área de informática evaluar la actualización a la versión más reciente de los productos Microsoft.
- Realizar la protección de los equipos y sistemas, asegurándose de que estas se encuentren actualizadas, con los parches de seguridad y de contar con un antivirus adecuado.
- Consultar con el experto en ciberseguridad o al encargado de informática a fin de tomar las medidas de protección si se presenta incidentes de seguridad digital.
- Extremar medidas de ciberseguridad.

Fuentes de información	▪ hxxps://thehackernews.com/2023/03/microsoft-rolls-out-patches-for-80-new.html