DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 064**	**Fecha: 15-03-2023**
		Página 22 de 25

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de elevación de privilegios de Microsoft Outlook		
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. **Resumen:**

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo exposición de información confidencial a un actor no autorizado que afecta al hash Net-NTLMv2 de Microsoft Outlook. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto Elevar privilegios y comprometer el sistema afectado.

2. **Detalles:**

- La vulnerabilidad de severidad **crítica** identificada como CVE-2023-23397, podría permitir a un atacante remoto a comprometer el sistema afectado. La vulnerabilidad existe debido a que la aplicación filtra el hash Net-NTLMv2. Un atacante remoto puede enviar un correo electrónico especialmente diseñado a la víctima y obtener el hash Net-NTLMv2 de la cuenta de Windows. La víctima no necesita abrir el correo electrónico, ya que la vulnerabilidad se activa automáticamente cuando el servidor de correo electrónico la recupera y procesa, por ejemplo, antes de que el correo electrónico se vea en el panel de vista previa.
- Los atacantes externos podrían enviar correos electrónicos especialmente diseñados que provocarán una conexión de la víctima a una ubicación UNC externa del control de los atacantes. Esto filtrará el hash Net-NTLMv2 de la víctima al atacante, quien luego puede transmitirlo a otro servicio y autenticarse como víctima. Esta vulnerabilidad se está explotando activamente en la naturaleza.
- La vulnerabilidad de tipo exposición de información confidencial a un actor no autorizado se debe a que el producto expone información confidencial a un actor que no está explícitamente autorizado para tener acceso a esa información.

3. **Productos afectados:**

- Microsoft Outlook: versión 2013 – 2021;
- Microsoft Office: versión 365 – 2021.

4. **Solución:**

- Microsoft recomienda actualizar los productos afectados con la última versión de software disponible que corrigen esta vulnerabilidad.

- Asimismo, recomienda agregar usuarios al grupo de seguridad de usuarios protegidos, lo que impide el uso de NTLM como mecanismo de autenticación. Cabe señalar, que realizar esta mitigación hace que la solución de problemas sea más fácil que otros métodos para deshabilitar NTLM. Se debe considerar usarlo para cuentas de alto valor, como administradores de dominio, cuando sea necesario. Se debe de tener en cuenta que esto puede afectar a las aplicaciones que requieren NTLM; sin embargo, la configuración se revertirá una vez que se elimine al usuario del grupo de usuarios protegidos.

- También, se debe bloquear el TCP 445/SMB saliente de su red mediante un firewall perimetral, un firewall local y mediante la configuración de su VPN. Esto evitará el envío de mensajes de autenticación NTLM a recursos compartidos de archivos remotos.

Fuentes de información	▪ hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23397