#MonikerLink: la vulnerabilidad de seguridad de Microsoft que pone en riesgo a los usuarios

16/02/2024

Microsoft Outlook se encuentra en el ojo de la tormenta luego de que una reciente investigación descubriera una importante **vulnerabilidad de seguridad**, conocida como **error #MonikerLink.**

La misma podría permitir que un atacante ejecute códigos en la máquina de la víctima, **robe datos privados** e instale **virus malware y ransomware** en los dispositivos.

El peligro es tal que, la misma empresa reconoció la vulnerabilidad. De hecho, la falla recibió una puntuación de gravedad de **9,8 sobre 10**, lo que da cuenta de la alarmante situación.

Cómo detectar la falla de seguridad y cuáles son sus consecuencias

A diferencia de otras aplicaciones, Outlook procesa hipervínculos que utilizan el protocolo **“file://”**, seguido de una ruta específica, un signo de exclamación y caracteres arbitrarios adicionales.

Estos hipervínculos manipulados **eluden los mecanismos de seguridad** existentes de Outlook, lo que podría incrementar el riesgo de filtración de **credenciales locales** y la posibilidad de ejecución de un **código arbitrario** que brinde acceso remoto al dispositivo.

Si se explota, esta vulnerabilidad podría permitir a los atacantes realizar una enorme variedad de **actividades maliciosas**, que incluyen:

- **Robo de datos:** acceder y extraer información confidencial almacenada en el sistema de la víctima o dentro de su red.
- **Instalación de malware**: implementar malware o registradores de pulsaciones de teclas, para comprometer aún más el sistema de la víctima o propagarse a través de una red.
- **Escalada de privilegios:** utilización de credenciales filtradas o ejecución de código arbitrario para obtener mayores privilegios en el sistema o la red de la víctima, lo que podría conducir a una toma de control total del sistema o de la red.
- **Robo de identidad:** utilizar credenciales robadas para hacerse pasar por la víctima, realizar actividades fraudulentas o acceder a recursos confidenciales.

Ciberdelito. Foto: Unsplash

Los especialistas **Check Point Research**, el equipo de de investigación que dio con esta falla, recomiendan a los usuarios aplicar los **parches y actualizaciones de seguridad** proporcionados por Microsoft, seguir las prácticas de ciberseguridad recomendadas para estos casos, permanecer atentos a hipervínculos y correos electrónicos desconocidos y **no hacer click** en enlaces sospechosos.

Fuente: Canal 26