ALERTA

Vulnerabilidad Crítica Microsoft Publisher (CVE-2024-38226)

COLCERT AL-1309-048

TLP:CLEAR

La vulnerabilidad crítica, identificada como CVE-2024-38226, es una omisión de funciones de seguridad que afecta a Microsoft Publisher. Ésta permite a los atacantes eludir las políticas de macros de Office, lo que les facilita ejecutar código malicioso, robar datos sensibles o comprometer sistemas completos. La explotación de esta vulnerabilidad puede tener graves consecuencias para la seguridad de los sistemas afectados, por lo que es crucial aplicar las actualizaciones y parches proporcionados por Microsoft.

Elementos de Inteligencia Disponibles

Un atacante debe estar autenticado en el sistema de destino y convencer a un usuario para que descargue un archivo especialmente diseñado. Esta explotación permite al atacante eludir las políticas de macros de Office, que están diseñadas para evitar la ejecución de archivos no confiables y potencialmente maliciosos. Es importante destacar que la vulnerabilidad no utiliza el panel de vista previa como vector de ataque, lo que significa que la explotación debe ocurrir a través de otros medios de interacción con archivos.

Análisis

La explotación exitosa de esta vulnerabilidad representa un riesgo significativo, ya que compromete las funciones de seguridad diseñadas para proteger a los usuarios de contenido dañino en Microsoft Publisher. Se recomienda a las organizaciones que utilizan Microsoft Publisher aplicar las actualizaciones de seguridad más recientes para mitigar los riesgos asociados con esta vulnerabilidad. Con un puntaje CVSS v3 de 7.3, se clasifica como crítica, lo que indica un alto riesgo de explotación

Recomendaciones

- ❑ Instalar las últimas actualizaciones de seguridad proporcionadas por Microsoft. La cual puede ser consultada en la Guía de Actualizaciones de Seguridad de Microsoft.
- ❑ Revisar y ajustar las políticas de macros en Office para asegurarte de que solo se ejecuten macros de fuentes confiables.
- ❑ Sensibilizar a los usuarios sobre los riesgos de abrir archivos de fuentes desconocidas y la importancia de seguir las políticas de seguridad.

NIVEL DE RIESGO

ALTO

FUENTES:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226
https://www.cve.org/CVERecord?id=CVE-2024-38226

COLCERT