BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-17
Fecha de publicación: 17/06/2024
Tema: Vulnerabilidad Zero Click en Outlook
Traffic Light Protocol (TLP): White

Producto(s) afectado:

Clientes de MS Outlook posteriores a la versión de 2016.

Descripción

El 11 de junio del 2024, Microsoft incluyó un parche dedicado a la vulnerabilidad denominada como CVE-2024-30103, que fue descubierta un mes anterior por los investigadores de Morphisec, con una puntuación severidad de 8.8

Esta vulnerabilidad fue descubierta el 3 de abril del 2024 y fueron reportados de manera privada a Microsoft. Los detalles por el momento no se divulgaron, sin embargo se sabe que se trata de una vulnerabilidad zero click, es decir, no requiere interacción del usuario; sin embargo, si es necesario que el correo que contiene el exploit sea abierto. La vulnerabilidad es más crítica en los entornos en los que está habilitada la función de apertura de correos automática, en cuyo caso la misma sería explotada sin necesidad de intervención del usuario.

Si el ataque es exitoso, se podrían inyectar DLLs maliciosos en los registros de Outlook, permitiendo tomar el control del equipo afectado.

No existe aún ningún exploit público para esta vulnerabilidad, sin embargo, los detalles técnicos serán revelados en agosto, por lo que es altamente probable que en poco tiempo se disponibilicen exploits, aumentando así la probabilidad de ataques.

Impacto

Un actor malintencionado que pueda explotar esta vulnerabilidad podría comprometer cualquier buzón y, por ende, lograr el control del sistema operativo subyacente.

Solución

Se recomienda a todos los usuarios que apliquen el parche denominado como “KB5002600” lo más pronto posible, pues este soluciona la vulnerabilidad.

Información adicional:

- https://borncity.com/win/2024/06/15/outlook-rce-vulnerability-cve-2024-30103-fixed-in-june-2024/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103
- https://blog.morphisec.com/cve-2024-30103-microsoft-outlook-vulnerability#/
- https://nvd.nist.gov/vuln/detail/CVE-2024-30103

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com