BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-59
Fecha de publicación: 30/10/2024
Tema: Vulnerabilidad persistente en Windows Themes
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Windows 10 y 11
- Windows Server 2012 hasta 2022

Descripción

El equipo de ACROS Security ha dado a conocer una nueva vulnerabilidad zero-day relacionada con un par que previamente se habían solucionado, la CVE-2024-38030 y CVE-2024-21320, la cual reside en el manejo de archivos de temas (.theme) en Windows. Cuando un usuario descarga o visualiza un archivo de tema que incluye imágenes ubicadas en una red compartida (a través de rutas UNC), el sistema intenta cargar automáticamente estas imágenes, lo que activa una autenticación NTLM hacia el servidor del atacante. Esto permite a un atacante capturar las credenciales NTLM del usuario y, potencialmente, descifrarlas o utilizarlas en ataques de retransmisión NTLM. La vulnerabilidad se explota sin necesidad de interacción significativa del usuario, más allá de visualizar el archivo en el Explorador de Windows.

Solución

Para mitigar el riesgo actualmente existen dos acciones a considerar, ya que Microsoft no ha lanzado un parche oficial para esta vulnerabilidad todavía:

- Deshabilitar NTLM en la configuración del sistema en aquellos entornos donde sea posible. Esta medida evita que el sistema realice la autenticación NTLM hacia servidores externos, mitigando el riesgo de que las credenciales sean interceptadas.

- Aplicar el parche no oficial de ACROS Security a través de la plataforma 0patch. Este micropatch implementa una solución en la memoria del sistema, lo que evita la necesidad de modificar la configuración del registro. La descarga y más detalles de

este parche están disponibles en el sitio oficial de 0patch, donde se pueden encontrar instrucciones de implementación.

Se recomienda evaluar estas medidas en función de la criticidad de los sistemas afectados, aplicando una o ambas mitigaciones hasta que se publique una actualización oficial de Microsoft.

Información adicional:

- Recurring Windows Flaw Could Expose User Credentials
- New Windows Themes zero-day gets free, unofficial patches
- Patching problems: The "return" of a Windows Themes spoofing vulnerability - Help Net Security

CYBOLT
Security Innovation

BEACON LAB
C S I R T

info@beaconlab.mx
beaconlab.mx
contact@cybolt.com
cybolt.com