BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-39
Fecha de publicación: 24/09/2024
Tema: CVE-2024-38014 Windows Installer Escalacion de Privilegios
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Windows 10, Windows 11, Windows Server 2008 y Windows Server 2012

Descripción

Una vulnerabilidad Zero-Day crítica, identificada como CVE-2024-38014 (CVSS 7.8), ha sido descubierta y parcheada recientemente, afectando a los instaladores MSI de Microsoft Windows. Esta vulnerabilidad permite la escalada de privilegios a SYSTEM, explotando las funciones de reparación de los instaladores MSI.

Los archivos MSI son ampliamente utilizados para instalar, actualizar y reparar software en sistemas Windows. Si bien la instalación y desinstalación requieren permisos elevados, las funciones de reparación pueden ser ejecutadas por usuarios con pocos privilegios. El problema reside en que estas reparaciones se ejecutan en el contexto de NT AUTHORITY\SYSTEM, lo que brinda acceso a altos niveles de control en el sistema. Esto permite a los atacantes aprovechar las ventanas de comandos que se abren durante la reparación de MSI para escalar sus privilegios y tomar control total de la máquina afectada.

Sin embargo, este ataque depende de la interfaz gráfica y condiciones específicas, como la presencia de ciertos navegadores, siendo más efectivos en Firefox y Chrome, mientras que Edge e Internet Explorer mitigan el riesgo.

Solución

Microsoft ha lanzado un parche como parte de sus actualizaciones de seguridad de septiembre de 2024 para mitigar esta vulnerabilidad. Este parche introduce un mensaje de Control de cuentas de usuario (UAC) cuando se ejecuta una función de reparación de MSI con privilegios elevados. Si el usuario rechaza la solicitud de UAC, el proceso se cancela, bloqueando el acceso no autorizado.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014

Información adicional:

- https://sec-consult.com/blog/detail/msi-installer-repair-to-system-a-detailed-journey/
- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-38014
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-38014

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com