I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Suplantación de interfaz de usuario (UI Spoofing) / Engaño al usuario
Nivel de riesgo: Media

II. ALERTA

Figura 1.- Vulnerabilidad Crítica de Suplantación de Interfaz (UI Spoofing) en Windows Shell (CVE-2026-32202)
Figura referencial

Microsoft ha revelado la explotación activa de una vulnerabilidad de tipo zero-click, identificada como CVE-2026-32202. Esta vulnerabilidad de UI Spoofing permite que un atacante no autorizado acceda a información confidencial del usuario de manera remota debido a un fallo en el mecanismo de protección de Windows Shell. El origen del problema está relacionado con un parche previamente liberado por Microsoft para tratar una vulnerabilidad de ejecución remota de código CVE-2026-21510, también en el mismo Windows Shell.

III. INTRODUCCIÓN

La interfaz de usuario que proporciona a los usuarios el acceso a una amplia variedad de objetos necesarios para ejecutar aplicaciones y administrar el sistema operativo,

Windows Shell, Microsoft fue alertada por la empresa de ciberseguridad Akamai, Dahan sobre la vulnerabilidad CVE-2026-32202 de ataque de suplantación de interfaz (UI Spoofing) a través de la red engañando al usuario mediante elementos visuales que aparentan ser legítimos del sistema operativo para obtener acceso a información sensible y confidencial del usuario.

Dahan también informo que tras la actualización de Microsoft a inicios del 2026 para corregir la vulnerabilidad de CVE-2026-21510 de protección para el propio Windows Shell, fue incompleta ya que persistió una falla de coerción de autenticación (CVE-2026-32202). Esta brecha entre la resolución de rutas y la verificación de confianza dejó un vector de robo de credenciales sin interacción del usuario (zero-click) mediante archivos LNK analizados automáticamente.

IV. VECTOR DE ATAQUE

La vulnerabilidad CVE-2026-32202 tiene un vector de ataque tipo RED, CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C con nivel de severidad 4.3 MEDIA.

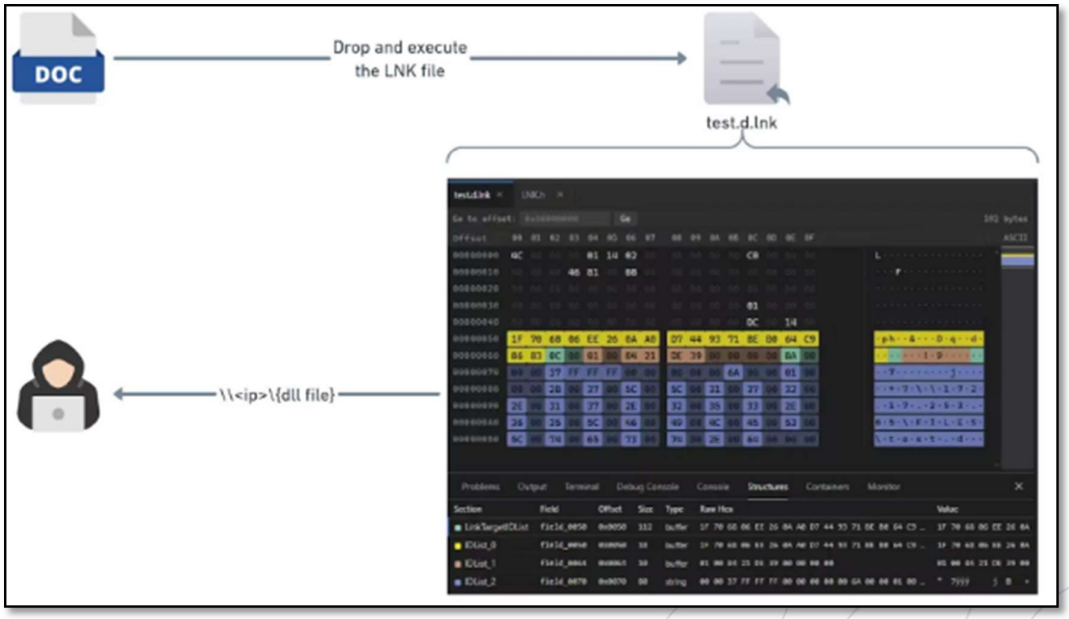

Figura 2.- Referencia de explotación de las vulnerabilidades CVE-2026-21510 y CVE-2026-32202 en Windows Shell (UI Spoofing).

Dahan informa también haber rastreado a un grupo del estado ruso llamado APT28 el cual dirigía sus campañas de explotación a Ucrania y las naciones de la UE a finales del 2025.

Para Dahan, el mecanismo de análisis de rutas (namespace parsing) de Windows Shell utilizado por APT28 permite cargar una biblioteca de enlace dinámico (DLL) desde un servidor remoto mediante una ruta UNC (Universal Naming Convention) para acceder a recursos compartidos como archivos, carpetas e impresoras en la red. La DLL se carga como parte de los objetos del Panel de Control (CPL) sin una validación adecuada de la zona de red.

En febrero de 2026, aunque se mitigó el riesgo de ejecución remota de código (habilitando Microsoft SmartScreen para verificar la firma digital y la zona de origen del CPL), aún se permitía que la máquina de la víctima se autenticara contra el servidor del atacante y descargara automáticamente el CPL.

Cuando la ruta es una ruta UNC (como '\\attacker.com\share\payload.cpl'), Windows inicia una conexión SMB hacia el servidor del atacante. Esta conexión SMB activa automáticamente un proceso de autenticación NTLM, enviando el hash Net-NTLMv2 al atacante, que posteriormente puede utilizarse para ataques de relay NTLM y descifrado offline.

V. IMPACTO

Campo	Detalle
Producto afectado	Microsoft Windows
Componente	Windows Shell
Fabricante	Microsoft
Versiones afectadas	Múltiples versiones de Windows (según boletines de seguridad)
Tipo de vulnerabilidad	Suplantación de interfaz (UI Spoofing – CWE-451)

Tabla 1.- Producto y versiones afectadas - Vulnerabilidad Crítica de Suplantación de Interfaz (UI Spoofing) en Windows Shell (CVE-2026-32202)

VI. INDICADORES DE COMPROMISO

- Recepción de archivos sospechosos provenientes de remitentes desconocidos.
- Ejecución de archivos con iconos o nombres engañosos (suplantación visual).
- Accesos anómalos a recursos locales tras la apertura de archivos o enlaces.
- Apertura de recursos desde ubicaciones remotas no confiables.

- Eventos inusuales en componentes del sistema como Windows Explorer o procesos del Windows Shell.
- Registros anómalos en:
  - Historial de ejecución de archivos recientes
  - Logs de ejecución del sistema (Shell)
  - Registros de seguridad del sistema (Security Event Logs)
- Archivos o accesos con apariencia aparentemente legítima pero comportamiento sospechoso.
- Reportes de usuarios sobre ventanas, mensajes o comportamientos engañosos del sistema.
- Actividad inusual posterior a la interacción con archivos, enlaces o ventanas emergentes.

VII. RECOMENDACIONES:

- Instalar de forma inmediata los parches publicados por Microsoft para corregir la vulnerabilidad en Windows.
- Habilitar actualizaciones automáticas para asegurar la instalación oportuna de futuras correcciones de seguridad.
- Informar a los usuarios sobre riesgos de ventanas falsas, prompts engañosos y solicitudes inusuales dentro del sistema operativo.
- Evitar interactuar con interfaces sospechosas y validar siempre el origen de ventanas emergentes rutas de ejecución (ej. procesos del sistema).
- Implementar y mantener actualizado software de protección (EDR/antivirus) que detecte comportamientos anómalos o intentos de spoofing.
- Aplicar el principio de mínimos privilegios para reducir el impacto en caso de explotación.
- Supervisar eventos relacionados con la ejecución de procesos inusuales y comportamientos anómalos en el entorno gráfico
- Validar la autenticidad de aplicaciones y componentes del sistema mediante firmas digitales.
- Evitar la ejecución de archivos o enlaces no confiables que puedan desencadenar la explotación del fallo.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

LINKEDIN (2026). Microsoft confirma la explotación activa de la vulnerabilidad CVE-2026-32202.https://es.linkedin.com/pulse/microsoft-confirma-la-explotaci%C3%B3n-activa-de-vulnerabilidad-cve-2026-32202-ifybe

NOTEBOOKCHECK (2026). Se confirma la explotación del día cero de Windows CVE-2026-32202.
https://www.notebookcheck.org/Se-confirma-la-explotacion-del-dia-cero-de-Windows-CVE-2026-32202.1285590.0.html

SECNEWS (2026). Microsoft Windows Shell Vulnerability CVE-2026-32202. https://www.secnews.gr/en/705386/microsoft-windows-shell-eupatheia/

THE HACKER NEWS (2026). Microsoft Confirms Active Exploitation of Windows Vulnerability CVE-2026-32202. https://thehackernews.com/2026/04/microsoft-confirms-active-exploitation.html