Boletín de alerta

Boletín Nro.:
Fecha de publicación: 02/03/2026
Tema: Alerta 2026-18 Vulnerabilidad CVE-2026-21513 en MSHTML bajo Explotación Activa
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Microsoft Windows 10
- Microsoft Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Descripción

Se identificó la vulnerabilidad **CVE-2026-21513** (CVSS 8.8), una falla de evasión de mecanismos de seguridad en el framework MSHTML. Esta vulnerabilidad fue explotada como **ZeroDay** antes de la publicación del parche y, de acuerdo con reportes de seguridad, **actualmente continúa siendo explotada activamente** en ataques reales.

MSHTML (componente mshtml.dll, también conocido con el nombre en clave Trident) es un componente de Internet Explorer que lleva a cabo las funciones de operatividad básica del navegador, en concreto, el filtrado y el renderizado de los documentos web, HTML, Hojas de estilo en cascada, entre otras funcionalidades. Asimismo permite integración con otras aplicaciones para Microsoft Windows mediante la exposición de una API de documento activo.

Investigaciones han vinculado la actividad de explotación con actores avanzados, incluido el grupo **APT28**.

La explotación ocurre cuando un usuario abre un archivo **HTML malicioso** o un acceso directo **(.lnk)** enviado por correo electrónico o descargado desde un enlace. Al abrirlo, el sistema puede omitir advertencias de seguridad y ejecutar contenido no autorizado, lo que podría permitir la ejecución de código y comprometer el equipo.

Indicadores de Compromiso

Los investigadores de Akamai han proporcionado los siguientes IOC:

Name	Indicator
document.doc.LnK	aefd15e3c395edd16ede7685c6e97ca0350a702ee7c8585274b457166e86b1fa
Domain	wellnesscaremed.com
MITRE Techniques	T1204.001, T1566.001

Solución:

Instalar inmediatamente la actualización de seguridad publicada por Microsoft.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513

Información adicional:

- https://thehackernews.com/2026/03/apt28-tied-to-cve-2026-21513-mshtml-0.html
- https://www.akamai.com/blog/security-research/2026/feb/inside-the-fix-cve-2026-21513-mshtml-exploit-analysis
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513