## I. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad de seguridad – Elusión de controles de seguridad

**Tipo de Incidente:** Bypass de mecanismos de seguridad en MSHTML Framework

**Nivel de riesgo:** Alta

## II. ALERTA


***Figura 1.-*** Vulnerabilidad CVE-2026-21513 en MSHTML Framework de Microsoft Windows - figura referencial

Se ha identificado una vulnerabilidad crítica en el MSHTML Framework de Microsoft Windows, catalogada como CVE-2026-21513, que permite a un atacante eludir controles de seguridad mediante el uso de contenido HTML o accesos directos manipulados.

La vulnerabilidad se encuentra activamente explotada y ha sido incluida por CISA en su catálogo de Known Exploited Vulnerabilities (KEV).

## III. INTRODUCCIÓN

El framework MSHTML de Microsoft (mshtml.dll) es el motor de renderizado HTML utilizado por Internet Explorer, aplicaciones de Microsoft Office y el modo Internet Explorer de Microsoft Edge.

Microsoft publicó un parche para una vulnerabilidad crítica de tipo 0-day identificada como CVE-2025-26153, clasificada como CWE-693 (Protection Mechanism Failure). Esta vulnerabilidad permite eludir mecanismos de seguridad del sistema mediante la apertura de archivos HTML o accesos directos (.lnk) especialmente diseñados, lo que podría derivar en la ejecución de código no autorizado.

## IV. VECTOR DE ATAQUE

La explotación requiere interacción del usuario, generalmente mediante técnicas de ingeniería social como campañas de phishing.

El atacante distribuye archivos HTML o accesos directos (.lnk) maliciosos que son procesados por Windows Shell en conjunto con MSHTML. Al abrir el archivo, el sistema puede omitir advertencias de seguridad y ejecutar contenido incrustado sin una validación adecuada.

No se requieren privilegios previos para su explotación. El vector de ataque es remoto y la vulnerabilidad posee una puntuación CVSS de 8.8 (Alta).

## V. IMPACTO

Los productos y versiones afectados son los siguientes:

| Producto | Versiones afectadas | Observaciones |
|---|---|---|
| Microsoft Windows 10 | Múltiples versiones soportadas | Incluye sistemas que mantienen el componente MSHTML para compatibilidad. |
| Microsoft Windows 11 | Versiones iniciales y actualizadas | Afectación asociada al uso del motor MSHTML (Trident). |
| Windows Server 2016 | Todas las ediciones soportadas | Exposición cuando MSHTML es invocado por aplicaciones o accesos directos. |
| Windows Server 2019 | Todas las ediciones soportadas | Riesgo presente en entornos de servidor con interacción de usuarios. |
| Windows Server 2022 | Todas las ediciones soportadas | Impacto condicionado al procesamiento de contenido HTML o archivos .lnk. |

| | | |
|---|---|---|
| Aplicaciones que integran MSHTML | Versiones dependientes | Software legacy que utilice MSHTML para renderizado HTML. |

***Tabla 1.-*** Productos y versiones afectadas - Vulnerabilidad CVE-2026-21513 en MSHTML Framework de Microsoft Windows

## VI. INDICADORES DE COMPROMISO

| Categoría | Indicador | Descripción |
|---|---|---|
| Archivo | HTML / .lnk sospechoso | Archivos HTML o accesos directos (.lnk) provenientes de fuentes no confiables abiertos por usuarios. |
| Registro de eventos | Actividad MSHTML | Eventos de sistema o aplicación que reflejen el uso anómalo del componente MSHTML o procesos asociados al renderizado web. |
| SIEM | Correlación de eventos | Alertas que vinculen la apertura de archivos sospechosos con la ejecución de procesos no habituales o encadenados. |
| EDR/XDR | Elusión de seguridad | Telemetría que evidencie intentos de bypass de controles de seguridad o ejecución no autorizada tras interacción del usuario. |

***Tabla 2.-*** Ioc- Vulnerabilidad CVE-2026-21513 en MSHTML Framework de Microsoft Windows

## VII. RECOMENDACIONES:

- Actualizar de forma prioritaria los sistemas Windows aplicando los parches de seguridad más recientes publicados por Microsoft, los cuales corrigen la vulnerabilidad CVE-2026-21513 y fallas asociadas en componentes del sistema operativo.
- Restringir el manejo de archivos potencialmente riesgosos en los servicios de correo electrónico y navegación web, en especial documentos HTML, accesos directos (.lnk) y otros formatos capaces de invocar el componente MSHTML.
- Fortalecer los controles preventivos frente a ingeniería social, habilitando advertencias de seguridad, validación de adjuntos y configuraciones de Políticas de Grupo que limiten la ejecución automática de contenido proveniente de orígenes no confiables.
- Concienciar a los usuarios sobre los riesgos de interactuar con archivos inesperados o provenientes de fuentes desconocidas, haciendo énfasis en enlaces, archivos HTML y accesos directos recibidos por correo o mensajería.
- Supervisar continuamente los registros y alertas de seguridad asociados al uso de MSHTML y a procesos de renderizado de contenido web, con el fin de identificar comportamientos anómalos que puedan indicar intentos de explotación.

## 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:

**NATIONAL VULNERABILITY DATABASE (NVD).** CVE-2026-21513: MSHTML Framework Security Feature Bypass Vulnerability**.**
https://nvd.nist.gov/vuln/detail/CVE-2026-21513

**MICROSOFT.** Security Update Guide – CVE-2026-21513 (Vendor Advisory)**.**
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513

**FEEDLY.** CVE-2026-21513 – Exploits & Severity Summary**.**
https://feedly.com/cve/CVE-2026-21513

**HISPASEC – UNA AL DÍA**. CISA advierte sobre seis nuevos 0-day críticos en Microsoft, incluyendo CVE-2026-21513**,** 2026.
https://unaaldia.hispasec.com/2026/02/cisa-advierte-sobre-seis-nuevos-0-day-criticos-en-microsoft-tras-explotacion-activa.html

**CVE DETAILS.** CVE-2026-21513 – Vulnerability Information**.**
https://www.cvedetails.com/cve/CVE-2026-21513/