Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 111	Fecha: 12-05-2023
		Página 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los expertos detallan la nueva vulnerabilidad de Windows Zero-Click para el robo de credenciales NTLM		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

Los investigadores de seguridad cibernética han compartido detalles sobre una falla de seguridad ahora parcheada en la plataforma MSHTML de Windows que podría abusarse para eludir las protecciones de integridad en las máquinas específicas.

DETALLES:

- La vulnerabilidad, rastreada como CVE-2023-29324 (puntaje CVSS: 6.5), ha sido descrita como una omisión de función de seguridad. Microsoft lo abordó como parte de sus actualizaciones de Patch Tuesday para mayo de 2023.
- El investigador de seguridad de Akamai, Ben Barnea, quien descubrió e informó el error, señaló que todas las versiones de Windows están afectadas, pero señaló que los servidores de Microsoft y Exchange con la actualización de marzo omiten la función vulnerable.
- Un atacante no autenticado en Internet podría usar la vulnerabilidad para obligar a un cliente de Outlook a conectarse a un servidor controlado por el atacante. Esto da como resultado el robo de credenciales NTLM. Es una vulnerabilidad de cero clics, lo que significa que puede activarse sin interacción del usuario
- También vale la pena señalar que CVE-2023-29324 es una omisión para una solución que Microsoft implementó en marzo de 2023 para resolver CVE-2023-23397 , una falla crítica de escalada de privilegios en Outlook que, según la compañía, ha sido explotada por actores de amenazas rusos en ataques dirigidos a entidades europeas desde abril de 2022.
- Esta vulnerabilidad es otro ejemplo más de revisión de parches que conduce a nuevas vulnerabilidades y omisiones. Es una superficie de ataque de análisis de medios sin clic que podría contener vulnerabilidades críticas de corrupción de memoria.

RECOMENDACIONES:

- Microsoft recomienda a los usuarios que instalen las actualizaciones acumulativas de Internet Explorer para abordar las vulnerabilidades en la plataforma MSHTML y el motor de secuencias de comandos.
- Mantener actualizado el Sistema operativo y software antivirus en las estaciones de trabajo.

Fuentes de información	▪ hxxps://thehackernews.com/2023/05/experts-detail-new-zero-click-windows.html ▪ Análisis propio de fuentes abiertas.

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 111**	**Fecha: 12-05-2023** **Página 5 de 13**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Microsoft lanzó actualizaciones de seguridad que corrige múltiples vulnerabilidades críticas y de día cero en varios de sus productos		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Microsoft ha lanzado nuevas actualizaciones de seguridad para MS Windows y MS Office, corrigiendo 38 vulnerabilidades, 2 de día cero (Zero-Day), 6 clasificadas como de severidad **CRÍTICA** y 32 de severidad **ALTA** de tipo ejecución remota de código, escalada de privilegios, suplantación de identidad (spoofing), divulgación de información, denegación de servicio y omisión de medidas de seguridad. Las vulnerabilidades que han sido catalogada como Zero-Day (día cero) están siendo explotadas activamente. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado.

2. **Detalles:**

- La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del mes de mayo, consta de 40 vulnerabilidades, calificadas como: 6 de severidad crítica, 32 altas y 2 de día cero.
- Microsoft indicó que han corregido tres vulnerabilidades de día cero de elevación de privilegios de Win32k registrada como CVE-2023-29336 que afecta a afecta a los sistemas que ejecutan Windows 10 y Windows Server 2008, 2012 y 2016, la vulnerabilidad de omisión de la función de seguridad de arranque seguro registrada como CVE-2023-24932 podría permitir que un atacante con acceso físico o privilegios administrativos ejecute código autofirmado en el nivel UEFI.
- Microsoft también resolvió la vulnerabilidad registrada como CVE-2023-24955, una falla de ejecución remota de código en SharePoint Server que fue revelada por el equipo de Star Labs en el concurso de exploits Pwn2Own Vancouver 2023.
- Las actualizaciones del martes de parches de mayo de 2023 de Microsoft abordan otros errores de elevación de privilegios y ejecución remota de código, junto con fallas de divulgación de información, denegación de servicio y omisión de funciones de seguridad.
- Las actualizaciones de Windows 10 y Windows 11 son acumulativas. El lanzamiento de seguridad mensual incluye todas las correcciones de seguridad para las vulnerabilidades que afectan a Windows 10, además de las actualizaciones que no son de seguridad. Las actualizaciones están disponibles a través del Catálogo de actualizaciones de Microsoft.

3. **Productos afectados:**

- Múltiples versiones de Microsoft Windows y Office.

4. Solución:

- Microsoft recomienda actualizar los productos afectados con la última versión de software disponible que aborda estas vulnerabilidades.
- En la página de Microsoft se informa de los distintos métodos para llevar a cabo dichas actualizaciones.

Fuentes de información	▪ hxxps://msrc.microsoft.com/update-guide/releaseNote/2023-May ▪ hxxps://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0373/ ▪ hxxps://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0372/ ▪ hxxps://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-mayo-de-2023