Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 110**	**Fecha: 11-05-2023**
		Página 4 de 21

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidades críticas RCE y dos Zero-Days en los parches de mayo de Microsoft		
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

La actualización de seguridad de Microsoft para mayo de 2023 es la más ligera desde agosto de 2021 con correcciones para un total de 49 nuevas vulnerabilidades, incluidas dos que los atacantes están explotando activamente.

La actualización incluye correcciones para nueve vulnerabilidades en el motor Chromium en el que se basa el navegador Edge de Microsoft. La empresa identificó siete de las 40 vulnerabilidades restantes como de gravedad crítica y el resto como "importantes".

DETALLES:

- Uno de los nuevos Zero-Day de este mes es una vulnerabilidad de escalamiento de privilegios de Win32k identificada como (CVE-2023-29336) que los atacantes pueden explotar para obtener el control completo de los sistemas afectados.

- Actualmente, no hay soluciones alternativas disponibles para la falla, lo que significa que la aplicación de parches es la forma más efectiva de mitigar el riesgo.

- El error, identificado como CVE-2023-24932, permite a un atacante eludir el arranque seguro e instalar una política de arranque de su elección. Un atacante necesitaría acceso físico o derechos administrativos en una máquina afectada para explotar la falla.

- En el caso CVE-2023-24932, el problema es grave porque el parche podría invalidar el firmware existente en la placa base. El parche completo implica actualizar el código de inicio de Microsoft en la partición de inicio de su disco duro y luego decirle a BIOS que ya no confíe más en el código de inicio antiguo e inseguro.

- Microsoft ha proporcionado un cronograma de tres etapas para esta actualización en particular:

    - Mayo 2023. El proceso manual completo descrito por Microsoft se puede usar para completar el parche hoy. Puede instalar el parche y no hacer nada más en este momento, lo que deja instalado el nuevo código de inicio y, por lo tanto, lista para aceptar la revocación descrita anteriormente, pero aún capaz de iniciar con los discos de recuperación existentes. Por supuesto, deja la vulnerabilidad aún explotable, porque el antiguo código de arranque todavía se puede cargar.
    - Julio 2023. Microsoft brindara herramientas de implementación automática más seguras. Presumiblemente, todas las descargas de instalación oficiales de Microsoft estarán parcheadas para entonces, por lo que incluso si algo sale mal, tendrá una forma oficial de obtener una imagen de recuperación confiable. En este punto, se podría completar el parche de forma segura y sencilla.
    - A principios de 2024. Los sistemas sin parches se actualizarán a la fuerza, incluida la aplicación automática de revocaciones criptográficas que evitarán que los medios de recuperación antiguos funcionen en su computadora, con lo que se espera cerrar el agujero CVE-2023-24932 de forma permanente para todos.

- Hay 12, de las vulnerabilidades que Microsoft reveló en su actualización de mayo de 2023 permiten la ejecución remota de código; ocho son fallas en la divulgación de información; y seis permiten a los atacantes eludir los controles de seguridad.

- Los RCE afectan el protocolo Network File System (NFS) de Microsoft para compartir archivos y acceso remoto a través de una red; la multidifusión general pragmática de Windows (PGM); Controlador Bluetooth de Windows; y el Protocolo ligero de acceso a directorios (LDAP) de Windows.

- Varios proveedores de seguridad identificaron un RCE en Microsoft NFS (CVE-2023-24941) como uno que las organizaciones deben priorizar debido al riesgo que presenta. Microsoft ha asignado al CVE una puntuación de gravedad de 9.8, la más alta en la actualización de mayo, debido a la baja complejidad de ataque asociada con el error y también al hecho de que no requiere la interacción del usuario. Un atacante con pocos privilegios podría explotar la falla en la red a través de una llamada no autenticada y especialmente diseñada a un servicio NFS.

- El SANS Internet Storm Center señaló a CVE-2023-28283, un RCE en Windows LDAP como otro error en el conjunto de mayo al que la organización debería prestar atención a pesar de que Microsoft mismo ha visto el error como menos probable de ser explotado. La vulnerabilidad brinda a los atacantes una forma de obtener RCE dentro del contexto del servicio LDAP a través de llamadas LDAP especialmente diseñadas.

- Un atacante no autenticado que explotara con éxito esta vulnerabilidad podría obtener la ejecución del código a través de un conjunto especialmente diseñado de llamadas LDAP para ejecutar código arbitrario dentro del contexto del servicio LDAP. Pero atacar la vulnerabilidad implica un alto grado de complejidad

- Una de las fallas críticas que Microsoft describió como más probable de ser explotada porque el código de prueba de concepto ya está disponible, es CVE-2023-29325, un RCE en la tecnología Windows Object Linking and Embedding (OLE). Un atacante puede desencadenar la falla al enviar un correo electrónico especialmente diseñado a una víctima y hacer que la víctima abra el correo electrónico con una versión afectada de Microsoft Outlook o simplemente lo vea en el panel de vista previa.

RECOMENDACIONES:

- Instalar las actualizaciones del fabricante disponibles en medios oficiales del proveedor. Para ello consulte con su personal técnico o áreas correspondientes.
- Revisar las soluciones alternativas que entrega Microsoft en cada uno de sus avisos de seguridad.
- Mantener actualizado el Sistema operativo y software antivirus en las estaciones de trabajo.

Fuentes de información	▪ hxxps://blog.segu-info.com.ar/2023/05/vulnerabilidades-criticas-rce-y-dos.html?m=1 ▪ Análisis propio de fuentes abiertas.