CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad en el navegador Microsoft Edge

Fecha: **14/10/2022**

Problemática: **Múltiples vulnerabilidades en los navegadores Microsoft Edge y Chrome**

Correlativo: **AA-0053**

Institución / Sector: **Instituciones Públicas y Privadas**

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alto**

CONTEXTO

Microsoft y Google han emitido un comunicado para informar a sus usuarios sobre las vulnerabilidades identificadas como CVE-2022-3450, CVE-2022-3449, CVE-2022-3447, CVE-2022-3446 y CVE-2022-3445, que afectan a los servicios Use after free in Skia, Heap buffer overflow in WebSQL, Inappropriate implementation in Custom Tabs, Use after free in Safe Browsing y Use after free in Peer Connection que afectan al software de los navegadores Microsof Edge y Chrome.

SITUACIÓN

El Centro Estratégico de Monitoreo – CEM, la vulnerabilidad clasificada como crítica fue encontrada en el servicio de sistema de eventos COM+ de Windows, que distribuye eventos automáticamente a los componentes del modelo de objetos componentes (COM). El servicio del sistema de eventos COM+ de Windows se inicia de forma predeterminada con el sistema operativo y es responsable de proporcionar notificaciones sobre los inicios y cierres de sesión. La explotación exitosa de esta vulnerabilidad permitirá a un atacante elevar los privilegios, ejecutar código arbitrario y realizar ataques de denegación de servicios en sistemas operativos windows.

Los detalles técnicos son desconocidos y un exploit no está disponible públicamente. La técnica de ataque empleada por esta falla es la T1068 según MITRE ATT&CK.

Recursos afectados:

- Microsoft Windows 7 y 8
- Microsoft Windows 10 (ver 1809,21H1, 21H2),
- Microsoft Windows 11

RECOMENDACIONES

Se recomienda a los usuarios de Sistemas Operativos de Microsoft Windows / Server realizar la actualización correspondiente de acuerdo a la versión que corresponda.

- Active las funciones de actualización automática de software en computadoras siempre que sea posible y pragmático.
- Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
- Los clientes que ejecutan una versión afectada de Microsoft Exchange deben habilitar la Protección extendida

DICCIONARIO DE DATOS

- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
- CVE (Common Vulnerabilities and Exposures); Listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad.
- Atacante (ciberdelincuente): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- DDOs Denial Of Service), es un Dos pero las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo, y más complicado de detener y determinar su origen.

REFERENCIAS

1. https://msrc.microsoft.com/update-guide/vulnerability
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41033
3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41033
4. https://attack.mitre.org/techniques/T1068/

ÁREA PARA DEFINICIONES