CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de seguridad

Fecha: **13/10/2022**

Problemática: **Múltiples vulnerabilidades en el navegador Microsoft Edge (basado en Chromium)**

Correlativo: **AA-0046**

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

CONTEXTO

Microsoft ha emitió un comunicado para informar a sus usuarios sobre las múltiples vulnerabilidades identificadas como CVE-2022-37996, CVE-2022-37995, CVE-2022-37991, CVE-2022-38039, CVE-2022-37990, CVE-2022-38038, CVE-2022-38037, CVE-2022-37988, CVE-2022-38022, CVE-2022-35761 que afectan al navegador Microsoft Edge (basado en Chromium) de Sistemas Operativos Windows.

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, un atacante puede llegar a explotar con éxito esta vulnerabilidad, y él tipo de información que podría revelarse es la almacenada en la memoria del kernel, el atacante podría leer el contenido de la memoria desde un proceso en modo usuario. Adicional a este acceso, el ciberdelincuente podría;

- **Escritura fuera de los límites en V8 (CVE-2022-3373)**
- **Usar después de gratis en Elementos personalizados (CVE-2022-3370)**
- **Validación insuficiente de entrada no confiable en Intents (CVE-2022-3317)**
- **Validación insuficiente de entrada no confiable en Navegación segura (CVE-2022-3316)**
- **Confusión de tipo en Blink (CVE-2022-3315)**
- **Interfaz de usuario de seguridad incorrecta en pantalla completa (CVE-2022-3313)**
- **Usar después de gratis en Importación (CVE-2022-3311)**
- **Aplicación de política insuficiente en pestañas personalizadas(CVE-2022-3310)**
- **Aplicación de políticas insuficiente en las herramientas para desarrolladores**
- **Usar después de gratis en Media (CVE-2022-3307)| CVE-2022-3304 Usar después de gratis en CSS**

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**

RECOMENDACIONES

Se recomienda a los usuarios de Sistemas Operativos de Microsoft Windows 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 para estar protegidos contra esta vulnerabilidad**

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**
- **Código arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.**
- **CVE (Common Vulnerabilities and Exposures); Listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad.**
- **Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputaciones mediante robo, filtrado de información.**

REFERENCIAS

1. https://msrc.microsoft.com/update-guide/vulnerability
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37996
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37995
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37991
5. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38022
6. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38039
7. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37990
8. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38038
9. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38037
10. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37988

ÁREA PARA DEFINICIONES