CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Suplantación de Identidad

Fecha: **10/10/2022**

Problemática: **Vulnerabilidad de suplantación de identidad de Microsoft Edge (basado en Chromium)**

Correlativo: **AA-0035**

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

CONTEXTO

Microsoft emitió un comunicado por medio de sus canales oficiales informando a sus usuarios sobre la vulnerabilidad identificada como CVE-2022-41035 que afecta al navegador de internet Microsoft Edge (basado en Chromium). La explotación de esta vulnerabilidad conlleva a un atacante a realizar una suplantación de identidad de su víctima.

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**	**Alto**	**Alto**

SITUACIÓN

Según la información obtenida por el Centro Estratégico de Monitoreo – CEM, Microsoft Edge (basado en Chromium) podría permitir que un atacante remoto realice suplantación de identidad, al persuadir a una víctima para que visite un sitio web especialmente diseñado, un atacante podría aprovechar esta vulnerabilidad para realizar un ataque de suplantación de identidad.

En un escenario de ataque basado en la web, un atacante podría alojar en un sitio web comprometido, un archivo especialmente diseñado para aprovechar la vulnerabilidad. Sin embargo, el atacante no tendría forma de obligar al usuario a visitar el sitio web. En su lugar, el ciberdelincuente tendría que convencer al usuario para que haga clic en un enlace, generalmente a través de un mensaje de correo electrónico o mensajería instantánea, y luego convencer al usuario para que abra el archivo especialmente diseñado.

Producto afectado:
Microsoft Edge (basado en Chromium) 106.0

REFERENCIAS

1. **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41035**
2. **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41035**

RECOMENDACIONES

- **El Centró Estratégico de Monitoreo-CEM recomienda a los usuarios de Microsoft Edge (basado en Chromium) ejecutar el parche de seguridad correspondiente lanzado por Microsoft apropiado para su sistema.**
- **Active las funciones de actualización automática de software en computadoras, teléfonos móviles y otros dispositivos conectados siempre que sea posible y pragmático.**
- **Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.**
- **Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos, clientes de correo electrónico y programas ofimáticos.**

DICCIONARIO DE DATOS

1. **Phishing: Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario.**
2. **Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo,**
3. **Vulnerabilidad:**
4. **Parche de seguridad: Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.**

ÁREA PARA DEFINICIONES