	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°275	Fecha: 17-11-2023
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en productos Fortinet		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo inyección de comando del sistema operativo e Inyección SQL en varios productos Fortinet. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la ejecución de código o comandos no autorizados.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-36553 de tipo inyección de comando del sistema operativo, podría permitir a un atacante remoto no autenticado ejecutar comandos no autorizados a través de solicitudes de API manipuladas.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-34991 de tipo inyección SQL, podría permitir a un atacante remoto no autenticado ejecutar consultas SQL no autorizadas a través de una solicitud HTTP maliciosa.

A. Productos afectados:

- FortiSIEM, versiones: 5.4.0, 5.3.3, 5.3.2, 5.3.1, 5.3.0, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.2, 5.2.1, 5.1.3, 5.1.2, 5.1.1, 5.1.0, 5.0.1, 5.0.0, 4.10.0, 4.9.0 y 4.7.2.
- FortiWLM, versiones: 8.6.5, 8.6.4, 8.6.3, 8.6.2, 8.6.1, 8.6.0, 8.5.4, 8.5.3, 8.5.2, 8.5.1, 8.5.0, 8.4.2, 8.4.1, 8.4.0, 8.3.2, 8.3.1, 8.3.0 y 8.2.2.

3. RECOMENDACIONES:

- Actualizar FortiSIEM a las siguientes versiones de software disponibles que abordan estas vulnerabilidades: versión 7.1.0, 7.0.1, 6.7.6, 6.6.4, 6.5.2, 6.4.3 o superiores).
- Actualizar FortiWLM a la versión 8.6.6, 8.5.5 o superior.

Fuente de Información:	• hxxps://www.fortiguard.com/psirt/FG-IR-23-135 • hxxps://www.fortiguard.com/psirt/FG-IR-23-142

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°275	Fecha: 17-11-2023
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Microsoft Edge		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

   Se ha reportado múltiples vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo uso después de la liberación, error de validación de entrada y ataque suplantación de identidad en Microsoft Edge. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario y comprometer el sistema vulnerable.

2. **DETALLES:**

   La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5997 y CVE-2023-6112 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación dentro del componente de recolección de basura y de navegación en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, provocar un error de uso después de la liberación y ejecutar código arbitrario en el sistema de destino.

   La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-36008 de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado con el navegador y ejecute código arbitrario en el sistema.

   Se ha asignado el siguiente identificador para la vulnerabilidad de severidad baja: CVE-2023-36026.

   A. Productos afectados:

   - Microsoft Edge: versión 79.0.309.71 - 119.0.2151.58.

3. **RECOMENDACIÓN:**

   - Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-5997 • hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-6112 • hxxp://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36008 • hxxp://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36026