DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°249**	**Fecha: 19-10-2023**
		Página: 8 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Apache HTTP Server		
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 **MEDIA** de tipo error de gestión de recursos y lectura fuera de límites en Apache HTTP Server. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS).

2. **DETALLES:**

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-45802 de tipo error de gestión de recursos, existe debido a una gestión inadecuada de los recursos internos dentro del servidor al manejar solicitudes HTTP/2. Un atacante remoto puede enviar múltiples solicitudes al servidor y realizar un ataque de DoS.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-43622 de tipo error de gestión de recursos, existe debido a una gestión inadecuada de los recursos internos dentro del servidor al procesar conexiones HTTP/2 con un tamaño de ventana de 0. Un atacante remoto puede agotar los trabajadores disponibles en el servidor y realizar un ataque de DoS.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-31122 de tipo lectura fuera límites, existe debido a una condición límite dentro del módulo mod_macro. Un atacante remoto puede enviar solicitudes especialmente diseñadas al servidor, desencadenar un error de lectura fuera de límites y realizar un ataque de DoS.

A. Productos afectados:

- Apache HTTP Server: versión 2.4.55 - 2.4.57.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxp://downloads.apache.org/httpd/CHANGES_2.4_2.4.58 • hxxps://www.cybersecurity-help.cz/vdb/SB2023101942

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°249	Fecha: 19-10-2023
		Página: 9 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Google ChromeOS		
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** de tipo uso después de la liberación, control de seguridad implementado incorrectamente para el estándar, validación de entrada incorrecta y condición de carrera en Google ChromeOS. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario, obtener acceso a información confidencial y comprometer el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5218 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación dentro del componente de aislamiento de sitios 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 **alta,** identificada por MITRE como CVE-2023-5475 de tipo control de seguridad implementado incorrectamente para el estándar, existe debido a una implementación incorrecta en DevTools en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5481 de tipo control de seguridad implementado incorrectamente para el estándar, existe debido a una implementación incorrecta en Descargas en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5479 de tipo control de seguridad implementado incorrectamente para el estándar, existe debido a una implementación incorrecta en la API de Extensiones en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad media y baja: CVE-2023-5476, CVE-2023-5485, CVE-2023-5478, CVE-2023-5486, CVE-2023-5473, CVE-2023-4921 y CVE-2023-21143.

A. Productos afectados:

- Sistema operativo Chrome: anterior a 118.0.5993.86

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2023/10/stable-channel-update-for.html