	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 134	**Fecha: 08-06-2023**
		Página 9 de 21

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Nueva vulnerabilidad de día cero identificada en el navegador Google Chrome		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

ANTECEDENTES:
El 06 de junio del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tomó conocimiento que Google lanzó actualizaciones de seguridad para reparar una falla de alta gravedad en su navegador web Chrome.

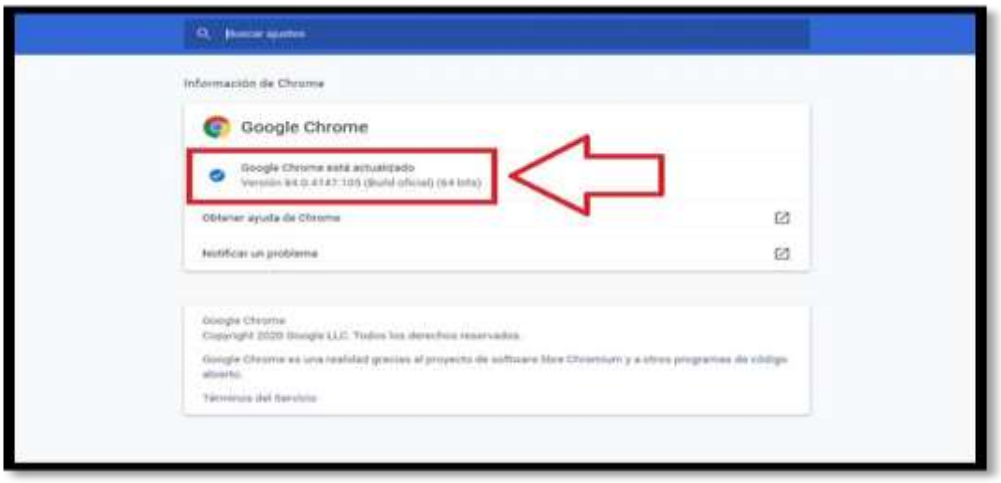
DETALLES:
Identificada con el código CVE-2023-3079, la vulnerabilidad se ha descrito como un error en el motor de JavaScript V8.

La confusión de tipos en V8 en Google Chrome antes de 114.0.5735.110 permitió a un atacante remoto explotar potencialmente la corrupción del montón a través de una página HTML manipulada, según la Base de datos de vulnerabilidad nacional (NVD) del NIST.

El gigante tecnológico, “Chrome” como suele ser el caso, no reveló detalles de la naturaleza de los ataques, pero señaló que está "consciente de que existe un exploit para CVE-2023-3079".

Con el último desarrollo, Google ha abordado un total de tres vulnerabilidades explotados activamente en Chrome desde el comienzo del año:

- CVE-2023-2033 (puntaje CVSS: 8.8) - Confusión de tipo en V8.
- CVE-2023-2136 (puntaje CVSS: 9.6) - Desbordamiento de enteros en Skia.



RECOMENDACIONES:
- Actualizar a la versión 114.0.5735.110 para Windows y 114.0.5735.106 para macOS y Linux para mitigar posibles amenazas.
- Aplicar correcciones que estén disponibles a los navegadores basados en Chromium como Microsoft Edge, Brave, Opera y Vivaldi que apliquen las correcciones a medida que estén disponibles.

Fuentes de información	hxxs://thehackernews.com/2023/06/zero-day-alert-google-issues-patch-for.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 134	Fecha: 08-06-2023
		Página 17 de 21

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica 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. **Resumen:**

   Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo confusión de tipos en Microsoft Edge. La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto ejecute código arbitrario en el sistema de destino.

2. **Detalles:**

   - La vulnerabilidad registrada con el código CVE-2023-3079 de severidad **crítica** de tipo desbordamiento de búfer, existe debido a un error de confusión de tipo dentro del motor V8 en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de confusión de tipo y ejecutar código arbitrario en el sistema de destino.

3. **Productos afectados:**

   - Borde de Microsoft: versión 79.0.309.71 - 114.0.1823.37.

4. **Solución:**

   - Se recomienda actualizar el paquete afectado con la última versión 4.2.6 disponible desde el sitio web del proveedor que aborda esta vulnerabilidad.

Fuentes de información	hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-3079