Nro. Alerta:	AL-2025-057	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	31-oct-2025	Vulnerabilidad Crítica - Motor de JavaScript V8 (Navegadores Chromium)	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad Crítica en Navegadores Web
Tipo de Incidente: Vulnerabilidad de Ejecución de Código Remoto (RCE)
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad Crítica - Motor de JavaScript V8 (Navegadores basados en Chromium) - figura referencial

CVE-2025-12036 es una vulnerabilidad que permite la ejecución remota de código (RCE) que se deriva de una implementación inapropiada dentro del motor JavaScript y WebAssembly V8 de los navegadores basados en Chromium.

III. INTRODUCCIÓN

V8 es el motor de JavaScript y WebAssembly de código abierto utilizado por navegadores como Google Chrome, Microsoft Edge, Opera y Brave para ejecutar el código JavaScript de las páginas web. Entre sus características principales se encuentran:

Seguridad: Incluye un entorno llamado V8 Sandbox, que aísla la ejecución del código JavaScript para proteger al usuario frente a ataques externos.

Rutas de entrada para la compilación Just-In-Time (JIT): V8 convierte el código JavaScript en código máquina mediante dos etapas principales:

- **Ignition:** Es el primer compilador. Recibe el Abstract Syntax Tree (AST) del código fuente JavaScript y lo transforma en bytecode, un lenguaje intermedio

de bajo nivel. Este se ejecuta rápidamente para iniciar la aplicación sin demoras.

- **TurboFan:** Funciona paralelamente a Ignition. Utiliza los datos de ejecución recopilados para optimizar el bytecode, traduciéndolo a código máquina nativo altamente eficiente, reemplazando así al código interpretado.

La vulnerabilidad CVE-2025-12036 permite la ejecución remota de código (RCE) en sistemas vulnerables al explotar estas rutas de entrada del motor V8, comprometiendo directamente la seguridad del navegador y, por ende, del sistema del usuario.

IV. VECTOR DE ATAQUE

Si bien Google no publica detalles de la explotación descubierta por su programa Big Sleep de Google, que es la iniciativa de investigación de ciberseguridad impulsada por la inteligencia artificial de la compañía, la define en CVSS:3.1 como vector de ataque de tipo RED, que se ejecuta desde el navegador con o sin la interacción del usuario, con una severidad: 9.8 Alta.

La vulnerabilidad CVE-2025-12036 estaría siendo relacionada con un manejo de tipo incorrecto o error lógico, ambas que han sido vías comúnmente usadas para escapar al Sandbox de V8 y generar ataques de ejecución remota de código como otras vulnerabilidades anteriores.

Esta falla al ser aprovechada por un atacante le permitiría engañar a los usuarios y hacer que visiten una página web especialmente diseñada con JS malicioso, lo que podría permitirles ejecutar código arbitrario dentro del proceso de renderizado del navegador.

V. IMPACTO

Los productos y versiones afectados son los siguientes:

- Motor de Javascript/WebAssembly V8 de los navegadores basados en Chromium.

VI. INDICADORES DE COMPROMISO

- Cualquier sitio o contenido web diseñado o infectado que contenga código JavaScript o WebAssembly malicioso.

- Google Chrome versión v137.0.7151.68/.69 o inferiores.

VII. RECOMENDACIONES:

- Actualizar Google Chrome a la versión 141.0.7390.122/.123
- Capacitar a los usuarios sobre los riesgos asociados al uso inseguro del navegador, como instalar extensiones desconocidas o acceder a enlaces no verificados.
- Forzar la instalación automática de actualizaciones en entornos corporativos, evitando excepciones que puedan dejar sistemas expuestos.
- Aplicar políticas de seguridad mediante GPO para restringir extensiones, bloquear sitios inseguros y habilitar características como sandboxing o aislamiento de procesos.
- Supervisar el comportamiento del navegador, prestando atención a conexiones anómalas, ejecución de WebAssembly sospechosa o módulos inusuales cargados por el navegador.
- Verificar manualmente que la versión actualizada del navegador esté instalada (revisando en "Acerca de"), asegurando que se haya aplicado el parche correspondiente a CVE-2025-12036.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

ECUCERT (2025). Vulnerabilidad Zero-Day — Google Chrome. https://www.ecucert.gob.ec/wp-content/uploads/2025/08/AI-2025-048-Vulnerabilidad-Zero-Day-%E2%80%94-Google-Chrome.pdf

TENABLE (2025). CVE-2025-12036 Detail. https://www.tenable.com/cve/CVE-2025-12036

SOC PRIME (2025). CVE-2025-12036 Vulnerability. https://socprime.com/blog/cve-2025-12036-vulnerability/

GOOGLE CHROME RELEASES (2025). Stable Channel Update for Desktop – October 21, 2025. https://chromereleases.googleblog.com/2025/10/stable-channel-update-for-desktop_21.html

SECURITY ONLINE (2025). Chrome Update: New High-Severity Flaw in V8 Engine (CVE-2025-12036). https://securityonline.info/chrome-update-new-high-severity-flaw-in-v8-engine-cve-2025-12036-requires-immediate-patch/