Nro. Alerta:	AL-2026-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	25-febrero-2026	Vulnerabilidad CVE-2026-2441 - Motor CSS de Google Chrome	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Permite a un atacante remoto ejecutar código arbitrario dentro de un entorno aislado a través de una página HTML diseñada
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- CVE-2026-2441: Vulnerabilidad Zero-Day en Chrome- Figura referencial
Fuente: https://ecosistemastartup.com/cve-2026-2441-vulnerabilidad-zero-day-en-chrome-guia/

La vulnerabilidad **CVE-2026-2441** representa el primer "Zero-Day" de alto impacto del año 2026 para el ecosistema Chromium. Descubierta por el investigador Shaheen Fazim y reportada el 11 de febrero de 2026, esta falla reside en el componente de hojas de estilo en cascada (CSS) del navegador. Debido a su naturaleza, permite a un atacante remoto ejecutar código no autorizado dentro del entorno restringido del navegador (*sandbox*), comprometiendo la integridad de la sesión del usuario.

III. INTRODUCCIÓN

La vulnerabilidad ha sido catalogada como un error de tipo **Use-After-Free (UAF)** (CWE-416) dentro del manejo de funciones de fuentes CSS (CSSFontFeatureValuesMap).

- **Puntuación CVSS:** 8.8 (Alta).
- **Componente Afectado:** Motor de renderizado de Google Chrome y navegadores basados en Chromium (Microsoft Edge, Brave, Opera, Vivaldi).
- **Versiones Vulnerables:** Versiones anteriores a la **145.0.7632.75/.76** en Windows y macOS, y anteriores a la **144.0.7559.75** en Linux.
- **Naturaleza del Fallo:** Se produce una invalidación de iteradores cuando el navegador intenta procesar valores de fuentes mientras el conjunto de datos está siendo modificado simultáneamente. Esto provoca que el sistema acceda a una posición de memoria que ya ha sido liberada, permitiendo la corrupción del "heap" (montículo de memoria).

IV. VECTOR DE ATAQUE

El ataque se clasifica como un escenario de **"Drive-by Download"** o ejecución remota basada en contenido web:

1. **Páginas HTML Maliciosas:** El atacante aloja una página web especialmente diseñada con código CSS corrupto.
2. **Interacción del Usuario:** La víctima solo necesita visitar el sitio web comprometido o hacer clic en un enlace malicioso (Phishing) para que el exploit se ejecute automáticamente.
3. **Inyección de Código:** Al procesar el CSS de la página, el navegador activa la vulnerabilidad UAF, lo que permite al atacante inyectar y ejecutar instrucciones arbitrarias dentro del proceso del navegador.

V. IMPACTO

Aunque el código se ejecuta inicialmente dentro del sandbox (aislamiento) de Chrome, el impacto es crítico:

- **Secuestro de Sesión:** El atacante puede robar tokens de autenticación y cookies de sitios abiertos en otras pestañas (banca, correo, redes sociales).
- **Exfiltración de Datos:** Acceso a la información que el usuario introduce en formularios o visualiza en el navegador.

- **Escalada de Privilegios:** Si se combina con otra vulnerabilidad del sistema operativo, el atacante podría "escapar" del navegador y tomar control total del equipo.

VI. INDICADORES DE COMPROMISO

Al ser una vulnerabilidad de nivel de aplicación (navegador), los IoCs pueden ser sutiles, pero se han identificado los siguientes patrones:

- **Comportamiento del Proceso:** Creación de procesos secundarios inusuales por parte de **chrome.exe o msedge.exe** (Por ejemplo: ejecución de PowerShell o CMD inmediatamente después de cargar una Web).

- **Tráfico de Red:** Conexiones salientes sospechosas hacia direcciones IP no categorizadas o dominios de mando y control (C2) tras la carga de un sitio web específico.

- **Artefactos en Memoria:** Inestabilidad del navegador o cierres inesperados (crashes) frecuentes al navegar por sitios con alta carga de estilos CSS personalizados.

- **Persistencia:** Modificaciones no autorizadas en el almacenamiento local del navegador (Local Storage) o en las cookies de sesión.

VII. RECOMENDACIONES:

- Actualizar Google Chrome a la versión 145.0.7632.75/.76 o superior. Es vital reiniciar el navegador tras la actualización, ya que el proceso en memoria sigue siendo vulnerable hasta que se cierra y se vuelve a abrir.

- Las organizaciones deben asegurar que navegadores secundarios como Microsoft Edge u Opera también sean actualizados, ya que comparten el mismo motor vulnerable.

- En entornos corporativos, forzar el reinicio automático de los navegadores cuando una actualización de seguridad esté disponible.

- Configurar las herramientas de detección y respuesta para alertar sobre ejecuciones anómalas originadas desde procesos de navegación web.
- Reforzar las campañas contra el Phishing, instando a los usuarios a no visitar enlaces de fuentes desconocidas, que es el método principal de entrega para este exploit.

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:

- **NIST (2026).** *CVE-2026-2441 Detail* https://nvd.nist.gov/vuln/detail/CVE-2026-2441
- **CVE (2026).** *Required CVE Record Information* https://www.cve.org/CVERecord?id=CVE-2026-2441
- **Google (2026).** *Chrome* Releases https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html
- **Ecosistema Startup (2026).** *CVE-2026-2441: Vulnerabilidad Zero-Day en Chrome [Guía]* https://ecosistemastartup.com/cve-2026-2441-vulnerabilidad-zero-day-en-chrome-guia//
- **REDDIT (2026).** *¿CVE-2026-2441 ya está parcheado en el paquete Chromium?*https://www.reddit.com/r/Fedora/comments/1r8wcrg/is_cve202662441_patched_in_chromium_package_yet/