Informe

Técnico

Vulnerabilidades Críticas Detectadas

COLCERT IN-20250604-023

TLP:CLEAR

El ColCERT ha identificado 5 vulnerabilidades de seguridad, clasificadas según su nivel de criticidad: 3 críticas, 1 alta y 1 media. Las fallas detectadas incluyen ejecución remota de código (RCE), escalamiento local de privilegios y exposición de dispositivos de red ampliamente utilizados. Este boletín presenta un análisis técnico detallado de cada caso, **incluye las técnicas MITRE ATT&CK asociadas, e incorpora recomendaciones prácticas para su mitigación, orientadas tanto a entornos corporativos como domésticos.**

Consolidado de Vulnerabilidades por Severidad

Criticidad	Número estimado	Descripción	Impacto
Críticas	3	Permiten control remoto sin autenticación	Compromiso total del sistema: ejecución remota de código, malware, caída de servicios.
Altas	1	Escalada de privilegios, evasión de controles	Acceso con privilegios elevados, alteración de configuraciones críticas, persistencia.
Medias	1	Configuración insegura, librerías obsoletas	Aumento de superficie de ataque, facilitación de ataques encadenados (XSS, RCE).

CVE	Producto	Tipo	Impacto	Acción recomendada
CVE-2025-4664	Google Chrome (Chromium)	Zero-day / RCE	Ejecución remota de código, evasión del sandbox	Actualizar a la versión 137.0.7151.41 (Build oficial) o superior
CVE-2025-4999	Linksys FGW3000	Inyección de comandos	Control total del dispositivo	Aplicar firmware versión 1.0.00.000015 (última publicada por Linksys)
CVE-2025-45513	Tenda FH451	Desbordamiento de pila	Ejecución de código sin autenticación	Utilizar firmware versión 1.0.0.9, o evaluar reemplazo si no hay actualizaciones recientes

Riesgo Operativo Asociado

Estas vulnerabilidades críticas permiten la ejecución remota de código y el control total de sistemas sin autenticación. Su explotación puede facilitar movimientos laterales, **instalación de malware y robo de datos en entornos corporativos, así como espionaje y acceso no autorizado en redes domésticas.**

Técnicas MITRE ATT&CK Asociadas (Críticas)

Técnica	Código	Descripción técnica	Ejemplo aplicado a la semana
Explotación de aplicaciones expuestas	T1190	Los atacantes aprovechan vulnerabilidades en servicios accesibles desde Internet.	Chrome vulnerable puede ser explotado al visitar una página maliciosa; routers Linksys expuestos a través del puerto WAN.
Intérpretes de comandos / scripting remoto	T1059	Uso de shells como bash, cmd, PowerShell o scripts JS para ejecutar payloads maliciosos.	Tras comprometer el router Linksys, el atacante ejecuta scripts de red para extraer datos o pivotear.
Inyección en procesos	T1055	El atacante inserta código malicioso en procesos legítimos en ejecución.	En Tenda FH451, un desbordamiento permite inyectar shellcode directamente en la memoria activa del firmware.
Evasión de controles de seguridad	T1202	Manipulación de configuraciones o explotación de debilidades en mecanismos de protección.	Chrome evade el sandbox del navegador, permitiendo al código malicioso interactuar directamente con el sistema operativo.

Vulnerabilidades Altas

CVE	Producto	Tipo	Impacto	Acción recomendada
CVE-2025-24076 / CVE-2025-24994	Windows 11	Escalada de privilegios	Control como SYSTEM en menos de 300 ms.	Instalar las actualizaciones acumulativas de mayo 2025 desde Windows Update.

Riesgo Operativo Asociado

Estas vulnerabilidades permiten a un atacante con acceso local (por ejemplo, tras explotar otra falla o mediante ingeniería social) elevar sus privilegios a nivel SYSTEM, el más alto en Windows. **Esto permite evadir controles, establecer persistencia en el sistema y moverse lateralmente en redes corporativas, comprometiendo activos críticos.**

Técnicas MITRE ATT&CK Asociadas (Altas)

Técnica	Código	Descripción técnica	Ejemplo aplicado a la semana
Escalada de privilegios	T1068	**Aprovechamiento de fallas en el sistema para obtener permisos elevados**	**Un atacante que accede al sistema como usuario estándar explota CVE-2025-24076 y obtiene acceso SYSTEM.**
Evasión de controles de seguridad	T1202	**Eludir restricciones impuestas por políticas del sistema o antivirus**	**La escalada permite desactivar defensas locales o instalar herramientas sin detección.**
Persistencia	T1547	**Modificación de componentes del sistema para ejecutar código al iniciar**	**Tras obtener privilegios, el atacante puede instalar puertas traseras o programas de espionaje.**

Vulnerabilidades Medias

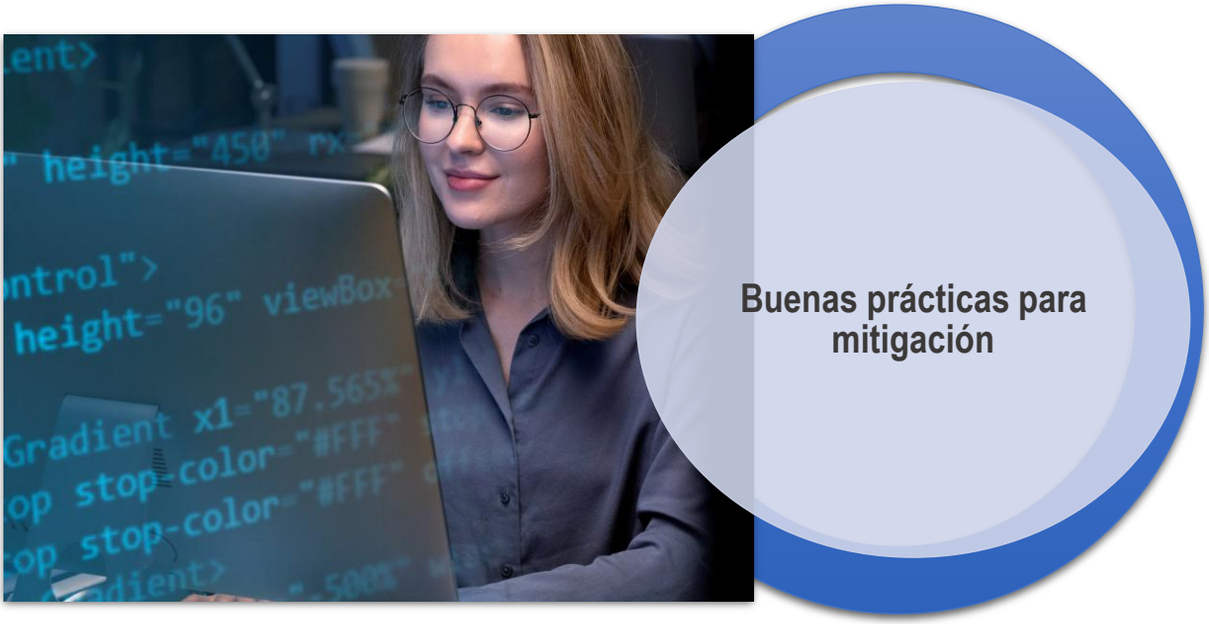
CVE	Producto	Tipo	Impacto	Acción recomendada
CVE-2025-5007	**Part-DB ≤ 1.17.0**	**XSS almacenado**	**Ejecución de scripts maliciosos en sesiones de usuarios administradores.**	**Migrar a la versión 1.17.1, implementar cabeceras CSP y sanitizar entradas de usuario.**

Riesgo Operativo Asociado

Aunque no permiten un compromiso directo del sistema, **las vulnerabilidades medias como esta aumentan la superficie de ataque.** El uso de código no validado en interfaces web puede facilitar el robo de sesiones, la alteración de configuraciones o la preparación de ataques dirigidos (phishing, movimiento lateral) en entornos mal protegidos.

Técnicas MITRE ATT&CK Asociadas (Medias)

Técnica	Código	Descripción técnica	Ejemplo aplicado a la semana
Captura de entradas (Input Capture)	T1056	**Interceptar datos de entrada del usuario a través de scripts u otras técnicas.**	**El XSS en Part-DB puede capturar cookies, tokens de sesión o campos de formularios.**
Abuso de librerías confiables	T1556.001	**Aprovechar dependencias de terceros mal gestionadas o no actualizadas.**	**Part-DB confía en funciones no sanitizadas del lado cliente, lo que permite inyección persistente.**
Explotación de interfaces web	T1190	**Abuso de formularios o vistas accesibles sin controles adecuados.**	**Un atacante malicioso crea un registro que inyecta JS y afecta al administrador al visualizarlo.**



Para **vulnerabilidades críticas** (Chrome, Linksys FGW3000, Tenda FH451).

- ❑ Aplicar versiones actualizadas en navegadores y firmware de routers. Verifica que sean versiones oficiales y revisa periódicamente si hay nuevas.
- ❑ Deshabilitar el acceso remoto innecesario en routers (por WAN) y restringir el acceso por IP o red segura.
- ❑ Usar navegación segura y aislamiento de procesos en navegadores, habilitando políticas como Site Isolation en Chrome.
- ❑ Segmentar la red doméstica/corporativa para evitar que un dispositivo comprometido (como un router) afecte otros activos críticos.
- ❑ Monitorear tráfico inusual desde navegadores o dispositivos IoT que puedan estar ejecutando código no autorizado.

Para **vulnerabilidades altas** (Windows 11 – escalada de privilegios).

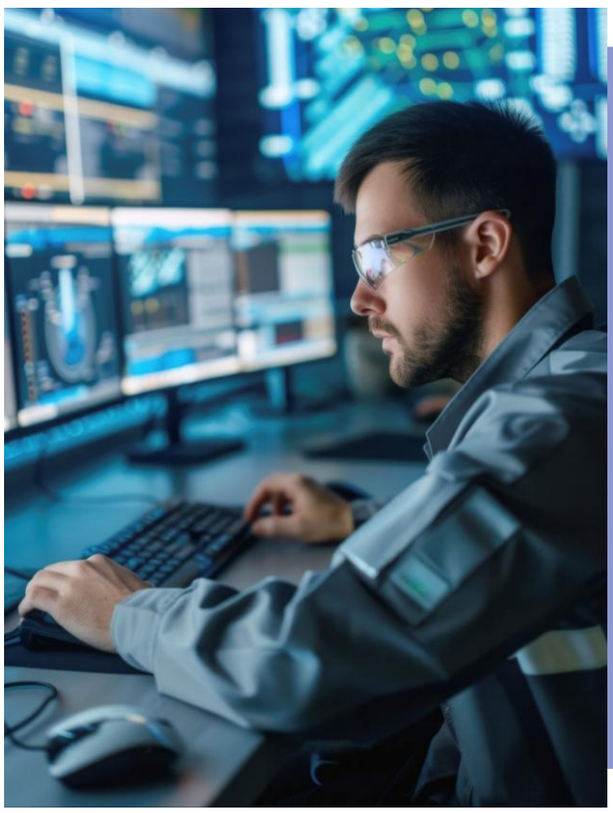
- ❑ Aplicar actualizaciones de seguridad del sistema operativo de forma automática y regular (Patch Tuesday).
- ❑ Restringir cuentas con privilegios administrativos y aplicar el principio de mínimo privilegio.
- ❑ Monitorear comportamientos anómalos en usuarios estándar, como ejecución de comandos privilegiados, con EDR o SIEM.

Para **vulnerabilidades medias** (Part-DB – XSS almacenado)

- ❑ Actualizar la aplicación a la última versión estable y segura.
- ❑ Implementar cabeceras de seguridad web (Content-Security-Policy, X-Content-Type-Options, X-Frame-Options).
- ❑ Validar y sanitizar todas las entradas del usuario, tanto en el lado cliente como en el servidor.
- ❑ Utilizar autenticación multifactor para proteger sesiones privilegiadas ante posibles robos de tokens.

Prácticas transversales recomendadas

- ❑ Realizar escaneos de vulnerabilidades periódicos.
- ❑ Habilitar monitoreo y alerta de eventos con herramientas SIEM (Wazuh, Splunk, ELK).).
- ❑ Educar a usuarios y equipos técnicos sobre amenazas como XSS, RCE y escalada local.
- ❑ Mantener inventario actualizado de activos para gestionar la exposición de software desactualizado o vulnerable.



Recomendaciones Finales

- ❑ Priorizar la mitigación de vulnerabilidades críticas detectadas.
- ❑ Fortalecer monitoreo y gestión de privilegios.
- ❑ Validar exposición de dispositivos conectados (routers, apps web).
- ❑ Aplicar actualizaciones de seguridad semanalmente.
- ❑ Continuar consultando boletines del ColCERT.

Sitios de fabricantes y desarrolladores:

Google Chrome Release Notes:
https://chromereleases.googleblog.com/
Detalles de la versión 137.0.7151.41 (actualización crítica para CVE-2025-4664).

Microsoft Security Response Center (MSRC):
https://msrc.microsoft.com/update-guide/
Detalles técnicos y parches relacionados con CVE-2025-24076 y CVE-2025-24994.

Linksys Support – Firmware & Advisories:
https://www.linksys.com/support/
Información de firmware vigente para modelos FGW3000.

Tenda Vulnerabilities – GitHub Report:
https://github.com/BenJpopo/V/blob/main/Tenda/FH451/
Análisis de vulnerabilidad de pila (CVE-2025-45513).

Part-DB GitHub Security Advisory:
https://github.com/advisories/GHSA-83qw-mxg2-hgpx
Publicación oficial del fallo de XSS en la versión 1.17.0.

Fuentes Oficiales

Bases de datos y catálogos de vulnerabilidades:

NIST National Vulnerability Database (NVD)
https://nvd.nist.gov/
Fuente técnica principal para la descripción detallada, puntajes CVSS y clasificación de todas las vulnerabilidades CVE incluidas en este boletín.

MITRE CVE System
https://cve.mitre.org/
Repositorio oficial de identificadores CVE. Proporciona trazabilidad estandarizada de cada vulnerabilidad y acceso a sus descripciones básicas.

CISA KEV Catalog (Known Exploited Vulnerabilities)
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Lista priorizada de vulnerabilidades con explotación activa confirmada. Referencia clave para determinar urgencia de mitigación (por ejemplo, CVE-2025-4664).

Zero Day Initiative (ZDI)
https://www.zerodayinitiative.com/advisories/published/
Plataforma de divulgación de vulnerabilidades descubiertas por investigadores independientes. Incluye hallazgos sobre productos como Google Chrome y dispositivos de red.