Informe

Técnico

Vulnerabilidades Críticas Detectadas
(24 al 30 de junio de 2025)

COLCERT IN-20250702-024

TLP:CLEAR

Durante la semana se identificaron **ocho vulnerabilidades de seguridad relevantes**, clasificadas según su criticidad en: **4 críticas, 3 altas y 1 media.** Estas vulnerabilidades afectan tanto aplicaciones web como componentes de hardware y herramientas de acceso remoto, e incluyen fallas como inyecciones SQL no autenticadas, corrupción de memoria, escalamiento de privilegios y cargas de archivos sin control. Este boletín presenta un análisis técnico detallado por severidad, **incluye las técnicas MITRE ATT&CK asociadas a cada caso, y proporciona buenas prácticas y recomendaciones concretas para su mitigación.**

Consolidado de Vulnerabilidades por Severidad

Criticidad	Nro.	Descripción	Impacto
críticas	4	Inyección SQL sin autenticación, bypass de login, ejecución remota de código.	Compromiso total del sistema, robo o manipulación de datos, ejecución de malware, persistencia.
Altas	3	Escalada de privilegios, evasión de controles	Acceso con privilegios elevados, alteración de configuraciones críticas, persistencia.
Medias	1	Falla en validación de entradas, XSS almacenado, malas prácticas en sesiones.	Superficie ampliada de ataque, robo de sesión, preparación de ataques encadenados.

Vulnerabilidades Criticas Identificadas

CVE	Producto	Tipo	Impacto	Acción recomendada
CVE-2025-6501	Inventory Management System (code-projects)	SQL Injection (múltiple)	Compromiso completo de base de datos	Actualizar versión y aplicar WAF
CVE-2025-52723	Inventory System	SQL Injection	Acceso no autorizado a datos	Parche urgente y validación de entradas
CVE-2025-6835	Library System	SQL Injection	Robo y alteración de registros	Revisar lógica de consultas y permisos
CVE-2025-6826	Payroll Management System	SQL Injection	Modificación de nómina/roles	Remediación inmediata en código y DB

Riesgo Operativo Asociado:

Las vulnerabilidades críticas identificadas afectan sistemas clave como inventarios, bibliotecas y nómina, y se relacionan con fallos de inyección SQL que permiten acceder y manipular bases de datos sin autenticación. Su explotación puede derivar en robo o modificación de información sensible, escalada de privilegios, movimientos laterales dentro de la red e interrupción de servicios. **Estas fallas representan un riesgo severo para la confidencialidad, integridad y disponibilidad de los datos, y pueden servir como punto inicial para ataques más amplios contra entornos corporativos o institucionales.**

Técnicas MITRE ATT&CK Asociadas (Críticas)

Técnica	Código	Descripción técnica	Ejemplo aplicado esta semana
Explotación para ejecución del cliente	T1203	Explotación de vulnerabilidades en aplicaciones para ejecutar código arbitrario	Uso de SQL Injection en sistemas de inventario y nómina (CVE-2025-6501, CVE-2025-6826).
Cuentas válidas	T1078	Abuso de credenciales válidas tras acceso no autorizado	Acceso a cuentas por medio de inyecciones que evaden autenticación (CVE-2025-52723).
Extracción de datos desde repositorios	T1213	Acceso no autorizado a bases de datos o sistemas para obtener información sensible	Robo de registros de bibliotecas y nómina (CVE-2025-6835, CVE-2025-6826).
Inyección SQL	T1505.001	Manipulación de consultas SQL para alterar o explotar estructuras de bases de datos	Inyección no autenticada en sistemas de gestión de inventarios.
Acceso a credenciales mediante aplicaciones web	T1557.003	Obtención de credenciales a través de formularios inseguros o APIs vulnerables	Exposición de acceso por validación deficiente en CVE-2025-52723.

Vulnerabilidad Alta con Explotación Activa (CISA KEV)

CVE	Producto	Tipo	Impacto	Acción recomendada
CVE-2025-3935	ConnectWise ScreenConnect	Bypass de autenticación.	Acceso remoto sin credenciales.	Aplicar actualización inmediata.
CVE-2025-27038	Qualcomm Adreno GPU	Corrupción de memoria.	Escalada de privilegios local.	Actualizar firmware o microcódigo.
CVE-2025-21479/80	Qualcomm GPU	Falta de validación de permisos.	Lectura/escritura indebida de memoria.	Actualización de drivers y políticas de acceso.

Riesgo Operativo Asociado:

Las vulnerabilidades detectadas impactan directamente herramientas de acceso remoto (ConnectWise ScreenConnect) y componentes de hardware críticos (GPU Qualcomm). Estas fallas permiten evadir mecanismos de autenticación, escalar privilegios mediante corrupción de memoria o acceder a zonas protegidas por validaciones deficientes. Su explotación facilita el acceso no autorizado, la alteración de la integridad de la memoria y la ejecución de acciones con privilegios elevados, comprometiendo la seguridad en entornos corporativos y dispositivos móviles. Son vectores altamente atractivos para atacantes por su bajo nivel de interacción requerida y su potencial de persistencia.

Técnicas MITRE ATT&CK Asociadas (Altas)

Técnica	Código	Descripción técnica	Ejemplo aplicado esta semana
Bypass de autenticación	T1556.001	Evasión de mecanismos de autenticación en aplicaciones o servicios	Acceso no autorizado en ConnectWise ScreenConnect (CVE-2025-3935).
Explotación de vulnerabilidad de hardware	T1203	Explotación de errores en firmware o controladores para escalar privilegios	Escalada de privilegios vía corrupción de memoria en GPU Qualcomm (CVE-2025-27038).
Manipulación de memoria	T1006	Lectura/escritura directa de memoria para evadir controles o robar información	Escritura indebida en memoria por falta de validación (CVE-2025-21479/80).
Ejecución con privilegios elevados	T1068	Uso de fallos en el sistema para ejecutar procesos con privilegios más altos	Ejecución arbitraria desde drivers vulnerables en entornos con GPU Qualcomm.

Vulnerabilidad Media de Alto Riesgo

CVE	Producto	Tipo	Impacto	Acción recomendada
CVE-2025-20282	Cisco Identity Services Engine (ISE)	File Upload no autenticado	Toma remota del sistema como root	Aislar, parchar, activar control de integridad

Riesgo Operativo Asociado:

Esta vulnerabilidad permite la carga de archivos no autenticada, lo que expone al sistema a una posible toma de control remoto con privilegios root. Esta falla representa un riesgo significativo pese a su clasificación media, ya que puede ser explotada sin interacción del usuario y habilita la ejecución arbitraria de comandos con los máximos privilegios. Su explotación compromete completamente la integridad y disponibilidad del sistema afectado, facilitando movimientos laterales, persistencia y la instalación de malware en entornos corporativos.

Técnicas MITRE ATT&CK Asociadas (Medias)

Técnica	Código	Descripción técnica	Ejemplo aplicado a la semana
Explotación de Aplicaciones Expuestas	T1190	Explotación de vulnerabilidades en aplicaciones accesibles desde internet, como interfaces web o APIs.	La vulnerabilidad en Cisco ISE permite la carga de archivos maliciosos sin autenticación previa.
Cuentas Válidas	T1078	Uso o creación de cuentas válidas para mantener el acceso persistente con privilegios elevados.	Un atacante podría crear o usar cuentas tras obtener control root del sistema comprometido.
Tareas o Trabajos Programados	T1053.005	Configuración de tareas programadas (cron, at) para mantener persistencia o ejecutar código malicioso.	Posible uso de cron jobs luego de la explotación para ejecutar scripts maliciosos.
Intérprete de Comandos y Scripts	T1059	Uso de intérpretes como Bash, PowerShell o similares para ejecutar comandos directamente en el sistema.	El atacante puede ejecutar comandos tras desplegar un web shell como root en el sistema.

Buenas prácticas para mitigación

Para vulnerabilidades críticas

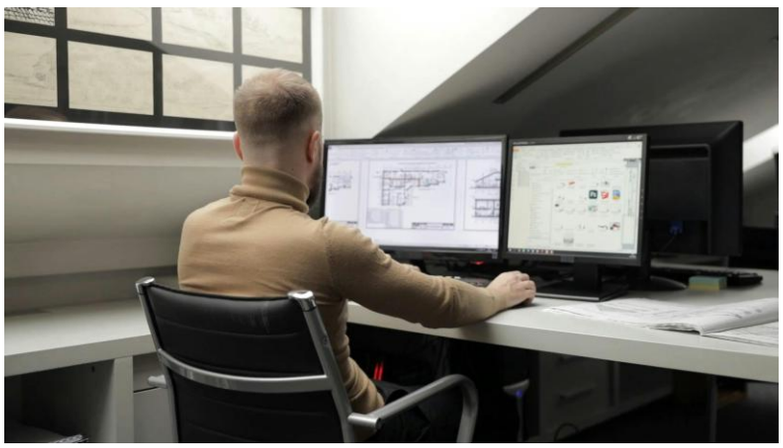
- ❑ Aplicar actualizaciones de seguridad de inmediato en todos los sistemas afectados.
- ❑ Implementar un firewall de aplicaciones web (WAF) para bloquear intentos de inyección SQL y explotación remota.
- ❑ Validar y sanitizar todas las entradas de usuario, especialmente en formularios web y consultas a bases de datos.
- ❑ Limitar privilegios de cuentas y aplicar el principio de mínimo privilegio en bases de datos y servicios críticos.
- ❑ Monitorear eventos de acceso y errores del sistema para detectar patrones anómalos o intentos de explotación.

Para vulnerabilidades altas

- ❑ Actualizar firmware, drivers y microcódigo de dispositivos afectados, especialmente en entornos móviles o BYOD.
- ❑ Restringir privilegios administrativos, evitando configuraciones por defecto o accesos innecesarios.
- ❑ Activar registros de auditoría y monitoreo continuo para detectar comportamientos anómalos (por ejemplo, escalada de privilegios).
- ❑ Implementar controles de acceso robustos, como autenticación multifactor (MFA) y segmentación de red.
- ❑ Validar políticas de seguridad a nivel de kernel o hardware, incluyendo configuraciones de GPU o gestión de memoria.

Para vulnerabilidades medias

- ❑ Actualizar firmware, drivers y microcódigo de dispositivos afectados, especialmente en entornos móviles o BYOD.
- ❑ Restringir privilegios administrativos, evitando configuraciones por defecto o accesos innecesarios.
- ❑ Activar registros de auditoría y monitoreo continuo para detectar comportamientos anómalos (por ejemplo, escalada de privilegios).
- ❑ Implementar controles de acceso robustos, como autenticación multifactor (MFA) y segmentación de red.
- ❑ Validar políticas de seguridad a nivel de kernel o hardware, incluyendo configuraciones de GPU o gestión de memoria.



Recomendaciones Finales

- ❑ Corregir de inmediato las vulnerabilidades críticas (SQLi, accesos remotos, etc.).
- ❑ Aplicar actualizaciones de software, firmware y microcódigo en sistemas afectados.
- ❑ Reforzar autenticación y permisos, limitando privilegios innecesarios.
- ❑ Validar entradas y aplicar WAF, CSP y controles contra ejecución remota.
- ❑ Monitorear con SIEM accesos anómalos y movimientos laterales.
- ❑ Aislar sistemas vulnerables hasta su corrección total.
- ❑ Ejecutar auditorías periódicas de seguridad y configuración.
- ❑ Capacitar al personal técnico en gestión segura y prevención de fallos.

Fuentes Oficiales

Bases de datos y catálogos de vulnerabilidades:

NIST National Vulnerability Database (NVD)
🔗 https://nvd.nist.gov/
Fuente principal de CVEs con detalles técnicos, puntajes CVSS y vectores de ataque.

MITRE CVE System
🔗 https://cve.mitre.org/
Repositorio oficial de identificadores CVE y sus descripciones estandarizadas.

CISA KEV Catalog (Known Exploited Vulnerabilities)
🔗 https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Lista priorizada de vulnerabilidades con explotación activa confirmada