

Durante esta semana se identificaron 20 vulnerabilidades de seguridad, clasificadas según su criticidad y potencial de explotación. Se detectaron fallas de ejecución remota de código (RCE), elevación de privilegios, y malas configuraciones de seguridad. **Este boletín resume los hallazgos más importantes y ofrece recomendaciones prácticas para mitigarlas.**

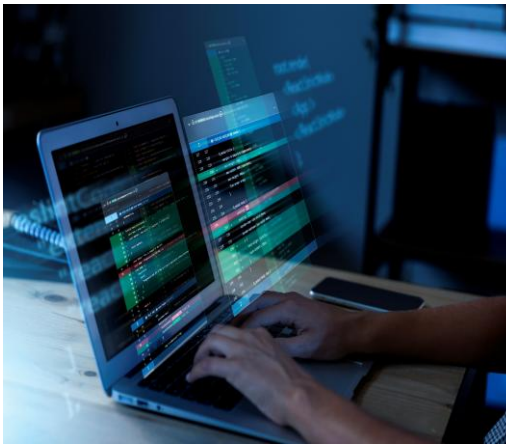
## Consolidado de Vulnerabilidades por Criticidad

| Criticidad | Número estimado | Descripción                                    | Impacto                                                                                                                                                     |
|------------|-----------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Críticas   | 8               | Permiten control remoto sin autenticación      | Compromiso total del sistema: permite ejecución remota de código, instalación de malware persistente, robo de credenciales o caída de servicios esenciales. |
| Altas      | 6               | Elevación de privilegios, evasión de controles | Acceso no autorizado con privilegios elevados, alteración de configuraciones críticas o establecimiento de persistencia en la red interna.                  |
| Medias     | 4               | Configuración insegura, librerías obsoletas    | Aumento de la superficie de ataque mediante malas configuraciones o librerías vulnerables; pueden facilitar ataques encadenados.                            |
| Bajas      | 2               | Exposición de información no sensible          | Exposición pasiva de información técnica o metadatos que facilitan fases de reconocimiento, phishing o escaneo automatizado.                                |

| CVE                    | Producto                   | Tipo                   | Impacto                                       | Recomendación                                        |
|------------------------|----------------------------|------------------------|-----------------------------------------------|------------------------------------------------------|
| CVE-2025-34028         | Commvault Web Server       | RCE                    | Control total del servidor                    | Actualizar a versiones 11.36.46, 11.32.89, 11.28.141 |
| CVE-2025-32432         | Craft CMS                  | RCE                    | Ejecución de comandos remotos y robo de datos | Actualizar a versiones 3.9.15, 4.14.15 o 5.6.17      |
| CVE-2025-0282          | Ivanti Connect Secure      | RCE Zero-day           | Instalación de DslogdRAT y acceso persistente | Aplicar parches oficiales de Ivanti                  |
| CVE-2025-34028 (var.)  | Commvault Command Center   | RCE                    | Compromiso del sistema                        | Instalar últimas actualizaciones de seguridad        |
| CVE-2025-30406         | CentreStack / Triofox      | RCE (deserialización)  | Ejecución de código arbitrario                | Aplicar hotfix del proveedor                         |
| CVE-2025-22457         | Ivanti Policy Secure / ZTA | RCE (buffer overflow)  | Control no autenticado del sistema            | Parchear de inmediato según advisory                 |
| CVE-2025-24813         | Apache Tomcat              | RCE (ruta de archivos) | Compromiso del servidor web                   | Actualizar a versión segura                          |
| CVE-2025-24252 + 24132 | Apple AirPlay              | RCE (Wi-Fi)            | Acceso sin interacción al dispositivo         | Actualizar firmware de Apple                         |

## Impacto:

Las vulnerabilidades críticas detectadas esta semana representan amenazas severas que permiten a los atacantes tomar el control total de sistemas mediante ejecución remota de código (RCE). Esto incluye el despliegue de malware persistente, robo de información confidencial y la interrupción de servicios esenciales. Algunas fallas como las de Ivanti y Apple permiten explotación sin autenticación previa o interacción del usuario, lo que incrementa significativamente el riesgo. La rápida explotación de estas vulnerabilidades por grupos de amenaza hace urgente la aplicación de parches y el refuerzo de controles perimetrales.



## Vulnerabilidades Altas Identificadas

| CVE            | Producto         | Tipo                    | Impacto                                       | Recomendación                             |
|----------------|------------------|-------------------------|-----------------------------------------------|-------------------------------------------|
| CVE-2025-31191 | macOS            | Escalada de privilegios | Evasión de sandbox, acceso extendido          | Aplicar parches de Apple (31/03/2025)     |
| CVE-2025-28933 | Linux sudo       | Escalada local          | Elevación de privilegios a root               | Actualizar sudo a última versión estable  |
| CVE-2025-26218 | PostgreSQL       | Inyección SQL           | Modificación o exfiltración de datos críticos | Actualizar motor de base de datos         |
| CVE-2025-28312 | Windows Defender | Evasión de detección    | Malware no detectado                          | Actualizar definiciones y motor AV        |
| CVE-2025-27548 | Cisco IOS XR     | Acceso no autenticado   | Compromiso de infraestructura de red          | Aplicar hotfix de Cisco                   |
| CVE-2025-26394 | FortiWeb         | CSRF                    | Manipulación remota de configuración          | Activar tokens CSRF y actualizar firmware |

### Impacto:



Estas vulnerabilidades permiten a actores maliciosos elevar privilegios, evadir controles de seguridad, inyectar comandos en bases de datos o comprometer dispositivos de red y seguridad perimetral. **La explotación puede dar lugar a accesos no autorizados, persistencia interna o manipulación de configuraciones críticas.** Son especialmente peligrosas cuando afectan entornos empresariales o dispositivos sin hardening adecuado, como routers o WAFs.

## Vulnerabilidades Medias

| CVE            | Producto         | Tipo                   | Impacto                                       | Recomendación                            |
|----------------|------------------|------------------------|-----------------------------------------------|------------------------------------------|
| CVE-2025-27783 | WordPress Plugin | XSS                    | Inyección de scripts maliciosos               | Eliminar o actualizar el plugin afectado |
| CVE-2025-29012 | jQuery v1.x      | Dependencia obsoleta   | Exposición a múltiples vectores XSS/RCE       | Migrar a jQuery ≥ 3.6                    |
| CVE-2025-26015 | Bootstrap <4.6   | Vulnerabilidad de UI   | Riesgos de Clickjacking y exposición de datos | Usar Bootstrap ≥ 5                       |
| CVE-2025-23482 | Aplicaciones web | Configuración insegura | Ausencia de headers de seguridad              | Implementar CSP, HSTS, XFO               |

### Impacto:



Las vulnerabilidades de severidad media están asociadas a malas prácticas de desarrollo y configuración, como la exposición de librerías obsoletas o la omisión de cabeceras de seguridad. Si bien no permiten por sí solas un compromiso inmediato, amplían la superficie de ataque y pueden ser utilizadas en conjunto con otras vulnerabilidades más críticas para comprometer aplicaciones o recolectar información útil para ataques dirigidos.

# Vulnerabilidades Bajas

| CVE            | Producto                 | Tipo                 | Impacto                                | Recomendación                             |
|----------------|--------------------------|----------------------|----------------------------------------|-------------------------------------------|
| CVE-2025-29945 | Cookies HTTP             | Sesiones inseguras   | Riesgo de secuestro de sesión          | Usar atributos HttpOnly, Secure, SameSite |
| CVE-2025-21994 | Servidores web genéricos | Información expuesta | Recolección pasiva de banners, headers | Minimizar información del servidor        |

## Impacto general:



Estas vulnerabilidades, aunque de impacto limitado por sí mismas, **permiten recolección pasiva de información, exposición innecesaria de datos de infraestructura o vectores que pueden ser aprovechados en fases de reconocimiento.** Si no se mitigan, pueden facilitar ataques posteriores mediante ingeniería social o scripts automatizados.

## ✓ Buenas Prácticas para Mitigación

- ❑ **Uso de herramientas de escaneo para detectar debilidades técnicas en infraestructura y aplicaciones.**

Implementar un proceso continuo y automatizado de gestión de parches, priorizando las vulnerabilidades críticas con explotación activa (como las listadas por CISA KEV). Verificar que todos los sistemas expuestos, especialmente servidores web, VPNs, firewalls y CMS, estén actualizados. Realizar pruebas previas en entornos controlados para evitar interrupciones.

- ❑ **Fortalecer las configuraciones de seguridad en aplicaciones web:**

Establecer políticas estrictas de cabeceras HTTP (Content-Security-Policy, Strict-Transport-Security, X-Frame-Options) y asegurar que las cookies incluyan los atributos HttpOnly, Secure y SameSite. Validar estas configuraciones con herramientas como SecurityHeaders.

- ❑ **Habilitar autenticación multifactor (MFA) en servicios sensibles:**

Implementar MFA en portales de acceso remoto (VPN, OWA, administración web), sistemas críticos y accesos de alto privilegio. Asegurar que los métodos MFA utilizados no sean susceptibles a ataques de SIM swapping o phishing (preferir tokens físicos o autenticadores basados en TOTP).

- ❑ **Realizar escaneos de vulnerabilidades de forma programada y bajo ciclo de mejora:**

Emplear herramientas como de escaneo para detectar debilidades técnicas en infraestructura y aplicaciones. Priorizar hallazgos según CVSS, criticidad del activo y exposición a internet. Complementar con pruebas de penetración controladas (pentesting).



### **Monitorear eventos en tiempo real con herramientas SIEM y EDR:**

Configurar correlaciones de eventos y reglas de alerta en SIEMs para detectar actividad anómala asociada a explotación de vulnerabilidades. Integrar soluciones EDR para respuestas automatizadas ante ejecución de comandos sospechosos o escalada de privilegios.

### **Fortalecer la capacitación del personal técnico y usuarios clave:**

Establecer programas continuos de formación en ciberseguridad, desarrollo seguro y respuesta ante incidentes. Simular ataques reales para preparar a los equipos ante escenarios críticos. Incluir campañas de concientización para usuarios administrativos y de TI.

### **Política de Contraseñas Robusta y Centralizada:**

Implementar normas obligatorias para el uso de contraseñas seguras (mínimo 12 caracteres con combinación de letras, números y símbolos) en todos los sistemas. Fomentar el uso de gestores de contraseñas seguros de código especialmente en cuentas administrativas o de sistemas críticos, evitando el almacenamiento inseguro de credenciales.

### **Eliminación de Servicios y Puertos Innecesarios:**

Realizar auditorías periódicas para identificar y deshabilitar servicios no utilizados o inseguros (por ejemplo: Telnet, FTP, SNMP v1/v2). Esta acción reduce la superficie de exposición y mitiga riesgos asociados a vectores comunes de ataque en infraestructuras mal configuradas.

### **Detección de Exposición Pública No Justificada:**

Utilizar herramientas de escaneo o scripts personalizados para identificar servicios y sistemas accesibles desde internet sin necesidad operacional. Documentar estos hallazgos y aplicar restricciones mediante listas blancas de IP, segmentación de red o reglas de cortafuegos.

### **Auditoría de Cuentas y Privilegios:**

Establecer un proceso trimestral de revisión de cuentas activas en sistemas críticos para identificar usuarios obsoletos, sin uso o con privilegios excesivos. Implementar controles que generen alertas ante la creación de cuentas con privilegios administrativos, evitando escalamiento no autorizado o persistencia encubierta.

# Técnicas MITRE ATT&CK Observadas



| Técnica                                                        | Código             | Descripción Técnica y Contexto                                                                                                                                                                                                                               |
|----------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exploit Public-Facing Application                              | T1190              | Explotación de aplicaciones accesibles desde Internet mediante vulnerabilidades en servicios como Apache Tomcat, Commvault Web Server y Craft CMS. Esta técnica permite a los atacantes inicializar la intrusión ejecutando código sin autenticación previa. |
| Command and Scripting Interpreter                              | T1059 (y subtechs) | Uso de intérpretes de comandos como bash, sh, cmd, PowerShell o Python para ejecutar payloads directamente en sistemas comprometidos. Observado especialmente en RCE como en Ivanti, donde se ejecutan comandos maliciosos vía consola.                      |
| Process Injection / Input Capture                              | T1055 / T1056      | Inyección de código en procesos legítimos (T1055) y captura de entradas (T1056), típicamente utilizadas tras una explotación para persistencia o evasión. Aplicable en explotación de deserialización en CentreStack o en malware como DslogdRAT.            |
| Exploitation for Privilege Escalation                          | T1068              | Explotación de vulnerabilidades locales en sistemas como macOS (CVE-2025-31191) o sudo en Linux para escalar permisos, evadir sandbox o acceder a funciones restringidas.                                                                                    |
| Abuse Elevation Control Mechanism: Trusted Developer Utilities | T1556.001          | Abuso de librerías o dependencias obsoletas (ej. jQuery, Bootstrap) como vector lateral. Puede incluir la manipulación de entornos web que confían en versiones inseguras para comprometer usuarios o inyectar scripts (XSS/RCE).                            |

## Fuentes Oficiales

 **CISA KEV Catalog (Known Exploited Vulnerabilities)**  
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

 **NIST National Vulnerability Database (NVD)**  
<https://nvd.nist.gov/>

 **Zero Day Initiative (ZDI)**  
<https://www.zerodayinitiative.com/advisories/published/>

 **Ivanti Security Advisories**  
<https://www.ivanti.com/support/security-updates>

 **Apache Tomcat – Security Vulnerabilities**  
<https://tomcat.apache.org/security.html>

 **Craft CMS – Seguridad y Boletines**  
<https://craftcms.com/security>

 **Apple Security Updates**  
<https://support.apple.com/en-us/HT201222>

 **Commvault Documentation and Vulnerability Information**  
<https://documentation.commvault.com/>