

Alerta

Actualización

Campaña de exfiltración de información

COLCERT AL – 20260306 - 097



Resumen Ejecutivo

El panorama de amenazas actual **evidencia que la exfiltración de información se está ejecutando mediante la explotación masiva de vulnerabilidades estructurales en activos web**, dejando de lado la utilización de ataques sofisticados (APTs).

De este modo, los atacantes logran comprometer información crítica con un esfuerzo mínimo, transformando cualquier vulnerabilidad no gestionada en una puerta de acceso inmediata.

El patrón dominante observado consiste en **el escaneo masivo de infraestructuras públicas para identificar tecnologías desactualizadas**, seguido de la explotación de vulnerabilidades conocidas (CVEs históricas) en aplicaciones web, sistemas de gestión de contenido (CMS) y plataformas de aprendizaje (LMS). Una vez logrado el acceso inicial, los atacantes proceden a la extracción de información para su posterior comercialización o divulgación en foros clandestinos.

Este escenario es crítico, ya que demuestra que la acumulación de problemas técnicos y la falta de mantenimiento continuo en los activos expuestos hacia Internet constituyen el vector de entrada principal, superando en frecuencia a técnicas más complejas. Además, se ha evidenciado que la explotación de infraestructuras tecnológicas compartidas o de proveedores de terceros representa un riesgo multiplicador, al permitir compromisos simultáneos a través de ataques a la cadena de suministro.



Análisis de riesgo inherente

Las evaluaciones de postura de seguridad en diversos sectores indican una exposición significativa y un riesgo elevado derivado de deficiencias sistémicas. Los hallazgos sugieren que una proporción considerable de organizaciones mantiene una postura reactiva o deteriorada frente a la gestión de vulnerabilidades.

El riesgo más inminente proviene de la operación de sistemas en estado End-of-Life (EOL). Se ha detectado el uso en producción de versiones de servidores web, lenguajes de programación y bibliotecas criptográficas que carecen de soporte de seguridad. Esto expone a las organizaciones a vulnerabilidades críticas, como la ejecución remota de código (RCE), falsificación de solicitudes del lado del servidor (SSRF) y lectura de memoria, para las cuales existen exploits públicos fácilmente automatizables. Estas brechas estructurales facilitan el acceso inicial y la exfiltración de datos.

NIVEL DE RIESGO

ALTO

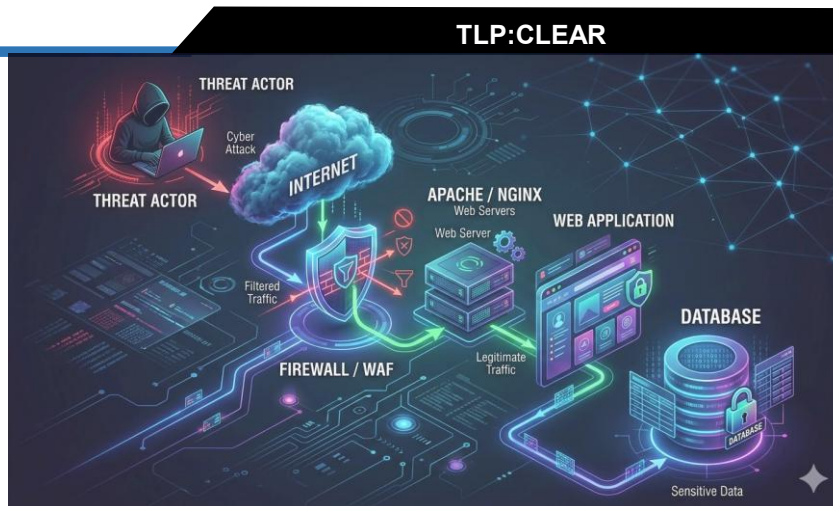


Figura 1. Arquitectura típica de servicios web expuestos (Apache/Nginx)



Tecnologías críticas vulnerables

- ❑ **Servidores web heredados:** riesgo sistémico en el uso de servidores web como Apache HTTP Server (EOL). Su presencia en entornos productivos expone a las organizaciones a vulnerabilidades de lectura de memoria, escalada de privilegios y ejecución remota de código con exploits.
- ❑ **Lenguajes de programación obsoletos:** el uso de versiones de PHP (EOL) introduce riesgos críticos. Estas versiones son susceptibles a fallos de inyección que pueden ser escalados a ejecución remota de código (RCE).
- ❑ **Bibliotecas criptográficas desactualizadas:** instancias de OpenSSL (EOL). Su uso compromete la confidencialidad e integridad de las comunicaciones al exponer los sistemas a fallos criptográficos conocidos y ataques de downgrade.
- ❑ **Plataformas LMS y CMS sin parches:** Sistemas de Gestión de Aprendizaje (LMS) y de Contenidos (CMS) son un objetivo principal cuando no se aplican parches de seguridad de forma inmediata. Vulnerabilidades de tipo Server-Side Request Forgery (SSRF), inyección SQL y Cross-Site Scripting (XSS) son explotadas para acceder a recursos internos y bases de datos.
- ❑ **Configuraciones inseguras de acceso y sesión:** la ausencia de atributos de seguridad en cookies (falta de HttpOnly y Secure), paneles administrativos expuestos directamente a Internet sin restricciones de IP, y servicios VPN o de escritorio remoto sin autenticación multifactor (MFA).
- ❑ **Falta de controles de identidad de dominio:** La ausencia de políticas DMARC y registros CAA, facilita la suplantación de identidad (spoofing) y la emisión fraudulenta de certificados.
- ❑ **Riesgos de cadena de suministro:** dependencia de scripts externos no verificados (ej. CDNs comprometidos) y vulnerabilidades heredadas a través de plataformas desarrolladas o alojadas por proveedores tecnológicos de terceros.

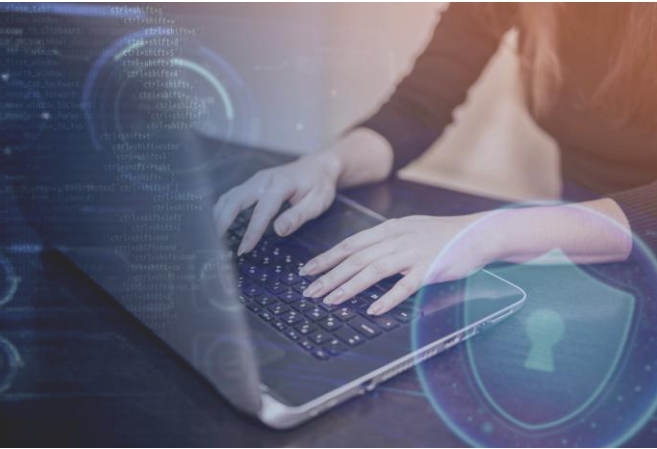
Matriz MITRE ATT&CK

Las tácticas, técnicas y procedimientos (TTPs) observadas se alinean con el siguiente patrón de ataque:

Táctica	ID	Técnica	Descripción del Comportamiento Observado
Reconocimiento	T1595	Escaneo Activo	Uso de herramientas automatizadas para escanear rangos de red en busca de software vulnerable y servicios expuestos.
Acceso Inicial	T1190	Explotación de Aplicaciones Públicas	Vector primario de compromiso mediante la explotación de vulnerabilidades conocidas (N-days) en aplicaciones web.
Colección	T1560	Archivo de Datos Recolectados	Los datos extraídos de las bases de datos son empaquetados y comprimidos antes de la exfiltración.
Exfiltración	T1041	Exfiltración Sobre Canal de C2	Los datos archivados son transferidos a infraestructuras controladas por el atacante a través de canales web.

Hipótesis: Escaneo automatizado

Se presume que los actores de amenaza emplean herramientas de escaneo masivo para identificar sistemáticamente infraestructuras que ejecutan versiones de software EOL. Una vez detectado un objetivo vulnerable, se despliegan exploits de forma automatizada para obtener acceso inicial. Esta metodología, centrada en vulnerabilidades conocidas, permite comprometer un gran número de objetivos con un esfuerzo mínimo, priorizando la velocidad y el volumen sobre la sofisticación del ataque individual.



Se presume que los actores de amenaza emplean herramientas de escaneo masivo para identificar sistemáticamente infraestructuras que ejecutan versiones de software EOL. Una vez detectado un objetivo vulnerable, se despliegan exploits de forma automatizada para obtener acceso inicial. Esta metodología, centrada en vulnerabilidades conocidas, permite comprometer un gran número de objetivos con un esfuerzo mínimo, priorizando la velocidad y el volumen sobre la sofisticación del ataque individual.

Validaciones de configuración críticas

- ❑ **Cifrados TLS débiles:** Validar que los protocolos obsoletos (SSLv3, TLS 1.0/1.1) y los conjuntos de cifrado débiles estén deshabilitados para prevenir ataques de interceptación y descifrado de tráfico.
- ❑ **Falta de banderas de seguridad en cookies:** Verificar que todas las cookies de sesión utilicen las banderas HttpOnly y Secure para mitigar el riesgo de secuestro de sesión (session hijacking) a través de ataques XSS y de interceptación de tráfico.
- ❑ **Exposición de paneles administrativos:** Asegurar que los paneles de administración de plataformas como WordPress, Joomla o Moodle no estén expuestos directamente a internet. Implementar controles de acceso por IP y autenticación multifactor (MFA).
- ❑ **Fugas de información del servidor:** Deshabilitar páginas de estado (/server-status) y directorios de diagnóstico (/Trace.axd) que exponen la configuración interna y facilitan el reconocimiento por parte de los atacantes.

Recomendaciones accionables para mejorar la postura de seguridad

Para mitigar estos riesgos de manera efectiva, se recomienda adoptar un enfoque de defensa en profundidad, priorizando la reducción de la superficie de ataque y la modernización de la infraestructura. Las siguientes acciones están estructuradas por prioridad de implementación:

NIVEL DE RIESGO

ALTO

Fase de Implementación	Acciones Estratégicas y Técnicas Recomendadas
Prioridad Inmediata	<ul style="list-style-type: none"> ▪ Identificar configuraciones inseguras en servidores web Apache/Nginx. ▪ Aplicar parches y actualizaciones de seguridad en sistemas y aplicaciones. ▪ Revisar configuraciones HTTP/HTTPS y encabezados de seguridad. ▪ Fortalecer controles de acceso a paneles administrativos. ▪ Activar y revisar registros de auditoría para detectar actividad anómala.
Prioridad Alta	<ul style="list-style-type: none"> ▪ Fortalecimiento de configuraciones: Deshabilitar protocolos TLS obsoletos (migrar a TLS 1.2+), asegurar cookies de sesión y ocultar información de diagnóstico o versiones de software en cabeceras HTTP. ▪ Protección perimetral: Implementar y afinar un Web Application Firewall (WAF) para bloquear intentos de explotación automatizada y escaneos maliciosos. ▪ Auditoría de proveedores: Evaluar la postura de seguridad de los proveedores tecnológicos que gestionan infraestructura compartida o aplicaciones tercerizadas. ▪ Seguridad de correo y dominio: Implementar políticas estrictas de DMARC, SPF, DKIM y registros CAA.

Fase de Implementación	Acciones Estratégicas y Técnicas Recomendadas
Prioridad Estratégica	<ul style="list-style-type: none"> ▪ Gestión continua de vulnerabilidades: Establecer un ciclo formal de escaneo, priorización y parcheo mensual. ▪ Autenticación robusta: Exigir Autenticación Multifactor (MFA) para todos los accesos administrativos, VPNs y portales transaccionales. ▪ Pruebas de seguridad: Ejecutar ejercicios periódicos de Pentesting sobre aplicaciones críticas y portales públicos. ▪ Monitoreo proactivo: Desplegar capacidades de inteligencia de fuentes abiertas (OSINT) para detectar tempranamente la exposición de credenciales o datos institucionales en foros clandestinos.

NIVEL DE RIESGO

ALTO

Beneficios de remediación enfocados en fortalecimiento estratégico

La implementación de estas recomendaciones contribuye a la mitigación de vulnerabilidades técnicas, aportando un valor estratégico fundamental para la resiliencia organizacional:

- ❑ Reducción drástica de la superficie de ataque: Al eliminar fallas técnica y asegurar las configuraciones, se neutralizan los vectores de ataque automatizados, obligando a los adversarios a invertir más recursos, lo que disuade a la mayoría de los actores oportunistas.
- ❑ Protección de la reputación y confianza: Prevenir la exfiltración de datos salvaguarda la confianza de los usuarios, ciudadanos y socios comerciales, evitando el daño reputacional a largo plazo asociado con la divulgación pública de información sensible.
- ❑ Cumplimiento normativo proactivo: El fortalecimiento de los controles de acceso y la protección de bases de datos asegura el cumplimiento de las leyes de protección de datos personales y normativas vigentes.
- ❑ Optimización de recursos de TI: La modernización de la infraestructura y la consolidación de sistemas reducen los costos operativos asociados al mantenimiento de plataformas heredadas y minimizan el impacto financiero de la respuesta a incidentes.
- ❑ Resiliencia ante ataques a la cadena de suministro: Al auditar y exigir estándares de seguridad a los proveedores tecnológicos, la organización se protege contra compromisos colaterales derivados de infraestructuras compartidas.

Como medida de apoyo frente a este panorama, aquellas entidades que no dispongan de capacidades propias para el análisis y gestión de vulnerabilidades pueden solicitar el acompañamiento del ColCERT. Para solicitar la realización de estos análisis sobre sus dominios, pueden contactarnos a través del buzón oficial: contacto@colcert.gov.co

En conclusión, las organizaciones que mantienen servicios web expuestos a Internet deben reconocer que configuraciones inseguras, vulnerabilidades en aplicaciones y controles de seguridad insuficientes pueden ser aprovechados por actores de amenaza para comprometer sistemas críticos y acceder a información sensible. La implementación oportuna de medidas de fortalecimiento, la gestión continua de vulnerabilidades y el monitoreo activo de la infraestructura son elementos clave para reducir el riesgo operativo. Adoptar una postura de seguridad preventiva y basada en buenas prácticas permitirá a las organizaciones mejorar su resiliencia frente a amenazas emergentes y proteger de manera efectiva sus activos digitales.



Fuentes

- ❑ Monitoreo de fuentes abiertas de información (OSINT).
- ❑ Cybersecurity and Infrastructure Security Agency (CISA).
- ❑ MITRE Corporation – Framework MITRE ATT&CK.
- ❑ National Institute of Standards and Technology (NIST).
- ❑ Google Threat Intelligence.
- ❑ SecurityScorecard.
- ❑ OWASP Foundation – Guías de seguridad para aplicaciones web.
- ❑ SANS Institute – Reportes y análisis técnicos.