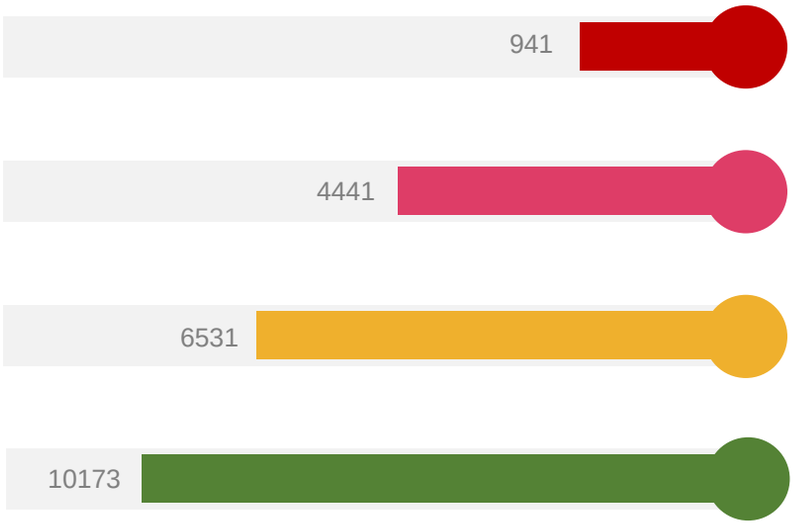
Informe

VULNERABILIDADES DETECTADAS 2024

COLCERT IN-20250505-019

TLP:CLEAR

- Sitios web
- Sistemas de información
- Aplicaciones
- Infraestructura



Fuente: ColCERT – Análisis de Vulnerabilidades 2024

Del total de las **22.086 vulnerabilidades**, se identificó que el 4,3% corresponden a Críticas, el 20,11% a Altas, el 29,57% a Medias y un 46,06% a Bajas, evidenciando **que las vulnerabilidades críticas, aunque pocas, suponen alto riesgo**.

Las **medias y bajas, por su volumen, amplían la superficie de ataque** y facilitan compromisos más complejos.

> “La identificación y gestión de vulnerabilidades es crucial para reducir riesgos y mejorar la postura de seguridad.”

> “Realizar planes de remediación de vulnerabilidades y revisar las configuraciones de seguridad de sitios web y portales es esencial para mantener una ciberseguridad efectiva.”

Es importante insistir en el diseño de planes que permitan identificar, priorizar y corregir vulnerabilidades, reduciendo el riesgo de ataques.

Además, las revisiones periódicas aseguran que los sitios web cumplan con los estándares actuales, protegiendo la integridad de los datos y la privacidad de los usuarios. Estas prácticas mejoran la seguridad y fomentan una cultura de concientización y responsabilidad al interior de entidades públicas y privadas.

COLCERT

Vulnerabilidades Críticas

Debilidades que pueden comprometer por completo un sistema, permitiendo a los atacantes tomar control total, robar información o interrumpir servicios esenciales. Entre ellas se encuentran:

Ejecución Remota de Código (RCE)

Permite a un atacante ejecutar comandos maliciosos en un servidor o aplicación sin necesidad de autenticación, comprometiendo su integridad.

Protocolos obsoletos SSL v2/v3

Versiones de cifrado inseguras que facilitan la intercepción de datos y ataques de intermediario (MITM).

Versiones no soportadas de PHP:

Software desactualizado con fallos conocidos que pueden ser explotados para infiltrarse en los sistemas.

Vulnerabilidades Altas

Fallos que facilitan accesos no autorizados y robo de datos, comprometiendo la confidencialidad y seguridad de la información.

Cross-Site Scripting (XSS)

Inyección de scripts maliciosos en sitios web vulnerables, permitiendo el robo de credenciales y manipulación de contenidos.

Inyección SQL

Ataques que explotan validaciones deficientes en bases de datos para acceder, modificar o eliminar información sensible

Escalada de privilegios

Vulnerabilidades que permiten a usuarios sin autorización obtener permisos administrativos en un sistema.

COLCERT

Vulnerabilidades Medias

Errores en configuraciones que aumentan la superficie de ataque y pueden ser utilizadas en conjunto con otras técnicas maliciosas.

Dependencias vulnerables)

Uso de librerías como Bootstrap y jQuery con fallos de seguridad conocidos que pueden ser explotados para tomar control de sitios web o aplicaciones.

Falta de cabeceras de seguridad (HSTS, CSP, X-Frame-Options)

Omisiones que permiten ataques como Clickjacking o la intercepción de datos.

Vulnerabilidades Bajas

Factores que, aunque de menor impacto por sí solos, pueden ser utilizados para ataques más sofisticados.

Cookies mal configuradas

Falta de atributos de seguridad como HttpOnly o Secure, exponiendo sesiones a secuestros.

Divulgación de información en encabezados HTTP inseguros

Exposición involuntaria de datos sensibles en respuestas del servidor, facilitando la recolección de información para ataques futuros.

Técnicas, Tácticas y Procedimientos utilizados (TTP)

Los ciberdelincuentes emplean diversas Tácticas, Técnicas y Procedimientos (TTP) para comprometer sistemas, robar información y evadir defensas. A continuación, se describen algunas de las más comunes e identificadas en la vigencia 2024.

Inyección de Código

Un atacante explota vulnerabilidades en aplicaciones para inyectar código malicioso. Técnicas como SQLi y XSS siguen siendo comunes para comprometer datos y alterar el funcionamiento del sistema.

Denegación de Servicio (DDoS)

Ataque que satura servidores o redes con tráfico excesivo, bloqueando el acceso a usuarios legítimos. Las variantes DDoS emplean múltiples dispositivos en red para aumentar la efectividad del sabotaje.

Ejecución remota de código (RCE)

La ejecución remota de código (RCE) permite a un atacante controlar un sistema sin acceso físico, explotando software vulnerable o mal configurado, lo que representa una amenaza crítica de seguridad.

Cross-Site Scripting (XSS): Ejecución remota de código (RCE)

Los ataques XSS inyectan scripts maliciosos en aplicaciones web vulnerables, permitiendo robar datos, secuestrar sesiones o redirigir usuarios. Son frecuentes en entornos como WordPress o jQuery sin codificación segura..

Configuraciones Débiles

Las configuraciones incorrectas exponen datos sensibles y permiten accesos no autorizados, facilitando ataques como Clickjacking, robo de sesiones o ejecución de código malicioso por falta de medidas básicas.

Uso de Software Obsoleto

El software desactualizado expone vulnerabilidades conocidas que pueden ser explotadas para comprometer sistemas. Librerías como Moment.js y Bootstrap requieren actualizaciones constantes para reducir estos riesgos.

Malas prácticas

Buenas Prácticas de Seguridad ante Amenazas Cibernéticas

Para salvaguardar la infraestructura digital, es esencial aplicar buenas prácticas de seguridad, como mantener actualizado el software crítico (PHP, Apache, WordPress), habilitar cabeceras de seguridad (HSTS, Content-Security-Policy) y desactivar protocolos antiguos (SSL v2/v3, TLS 1.0/1.1). Además, implementar monitoreo proactivo con herramientas de escaneo y análisis permite detectar vulnerabilidades a tiempo, donde **la capacitación continua del equipo en ciberseguridad es fundamental para minimizar errores humanos y reforzar la defensa** contra posibles amenazas cibernéticas.

Actualizar software crítico como PHP, Apache y WordPress

Utilizar versiones soportadas y mantenidas.

Configurar sistemas para aplicar actualizaciones automáticamente cuando sea posible.

Consultar las notas de seguridad oficiales de cada proveedor antes de actualizar en producción.

Habilitar cabeceras de seguridad como HSTS y Content-Security-Policy

Estas cabeceras fortalecen la protección del navegador contra ataques comunes. Implementa:

- `Strict-Transport-Security` para forzar HTTPS.
- `Content-Security-Policy` para restringir fuentes de scripts.
- `X-Frame-Options` para prevenir Clickjacking.

Verifica con herramientas como securityheaders.com.

Implementar monitoreo proactivo con herramientas de escaneo y análisis.

Utilizar escáneres como OpenVAS, Nessus o Nikto para detectar vulnerabilidades. Integra SIEMs para monitoreo en tiempo real y define alertas para eventos críticos.

Desactivar protocolos antiguos como SSL v2/v3 y TLS 1.0/1.1

Configurar tu servidor web o proxy inverso para soportar solo TLS 1.2 y TLS 1.3. Esto evita ataques como POODLE o BEAST. Ejemplo en Apache:

```
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

COLCERT

Tendencias de Ciberamenazas en Colombia: Fallas Comunes y Riesgos Críticos en 2024

En el 2024, el panorama de vulnerabilidades identificadas, evidencia una situación alarmante, caracterizada por la persistencia de configuraciones inseguras, el uso de software desactualizado y la explotación de dependencias vulnerables en plataformas críticas.

Las vulnerabilidades asociadas a **ejecución remota de código (RCE)** y **técnicas de inyección de código** como **SQLi** y **XSS** continúan encabezando los hallazgos, lo que refleja una preferencia por vectores de ataque que permiten a los actores maliciosos comprometer sistemas de manera completa y remota.

Por otro lado, la ausencia o configuración incorrecta de cabeceras de seguridad como **HSTS**, **X-Frame-Options** y **Content-Security-Policy** sigue siendo un problema recurrente. Esta omisión incrementa la exposición a ataques como el **Clickjacking** y redirecciones maliciosas.

A ello se suma el uso continuo de **protocolos obsoletos** y **algoritmos de cifrado débiles** en SSL/TLS, lo cual pone de manifiesto deficiencias significativas en la actualización de la infraestructura tecnológica.

En cuanto al impacto, si bien las **vulnerabilidades críticas** son menos frecuentes, representan un riesgo elevado por su potencial de comprometer activos sensibles. Las **vulnerabilidades de severidad media y baja**, aunque más comunes, amplían la superficie de ataque y suelen ser la vía de entrada para comprometer sistemas en ataques más complejos y dirigidos.

Estos hallazgos resaltan la necesidad de adoptar estrategias de **seguridad proactiva**, enfocadas en la actualización continua de componentes, la mejora de configuraciones de seguridad y la reducción de riesgos asociados a dependencias vulnerables, con el fin de hacer frente a un entorno de amenazas cada vez más sofisticado y dinámico.