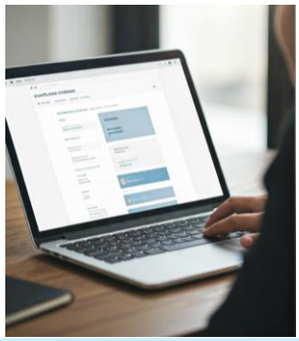
Advertencia de Seguridad

Vulnerabilidades comunes de los sistemas de gestión de contenidos (CMS)

COLCERT AD-2009-019

TLP:CLEAR



Los sistemas de gestión de contenidos (CMS) son herramientas esenciales para la creación y administración de sitios web, permitiendo a los usuarios crear, editar y publicar contenido web sin necesidad de conocimientos de programación. Sin embargo, también son vulnerables a diversas amenazas cibernéticas. A continuación, se presentan las vulnerabilidades comunes que deben ser consideradas para evitar explotaciones.

Vulnerabilidades en los CMS:

Inyección de código:
La inyección de código es un ataque en el que un atacante inserta código malicioso en un sitio web, lo que puede llevar a la ejecución no autorizada de comandos o la manipulación de datos. Este tipo de vulnerabilidad es frecuente y puede tener consecuencias graves para la integridad del sitio.

Cross-Site Scripting (XSS):
El XSS permite a los atacantes ejecutar scripts en el navegador de los usuarios, lo que puede resultar en el robo de información sensible, como cookies o credenciales. Este ataque se basa en la ejecución de código desde el navegador en lugar del servidor, lo que lo hace especialmente peligroso.

Falsificación de peticiones entre sitios (CSRF):
Este tipo de ataque engaña a los usuarios para que realicen acciones no deseadas en aplicaciones web donde están autenticados. Por ejemplo, un atacante puede hacer que un usuario envíe una solicitud que cambia su contraseña sin su conocimiento.

Plugins vulnerables:
El uso de plugins desactualizados o no seguros puede introducir vulnerabilidades en el CMS. Es fundamental mantener todos los componentes del sistema actualizados y eliminar aquellos que no se utilizan.

Vulnerabilidades Específicas por CMS:

- **WordPress:** Representa aproximadamente el 28% de los sitios comprometidos, siendo uno de los CMS más atacados debido a su amplia adopción y a la cantidad de plugins disponibles que pueden no estar actualizados.
- **Joomla:** Con un 9% de sitios comprometidos, también es un objetivo común para los atacantes.
- **Drupal:** Aunque representa solo el 1% de los sitios comprometidos, sigue siendo vulnerable si no se mantiene adecuadamente.

Contraseñas débiles:
Las contraseñas poco seguras son una puerta abierta para los atacantes. Es crucial implementar políticas de contraseñas robustas y fomentar el uso de combinaciones complejas y únicas para cada usuario.

Mejores Prácticas de Seguridad:

Actualizaciones regulares: Mantener el CMS, así como todos los plugins y temas, actualizados es crucial. Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades conocidas. Se recomienda aplicar estas actualizaciones tan pronto como estén disponibles para minimizar el riesgo de explotación por parte de atacantes.

Uso de contraseñas seguras: Implementar políticas de contraseñas robustas es esencial. Las contraseñas deben ser complejas, únicas y cambiadas regularmente. También se sugiere la utilización de autenticación de dos factores (2FA) para añadir una capa adicional de seguridad al acceso administrativo.

COLCERT

Advertencia de Seguridad

Vulnerabilidades comunes de los sistemas de gestión de contenidos (CMS)

COLCERT AD-2009-019

Copias de seguridad periódicas: Realizar copias de seguridad regulares garantiza que se pueda restaurar el sitio en caso de un ataque exitoso o pérdida de datos. Estas copias deben almacenarse en ubicaciones seguras y ser fácilmente accesibles.

Restricción de permisos: Limitar los permisos de usuario a lo estrictamente necesario reduce el riesgo de accesos no autorizados. Es importante revisar periódicamente los roles y permisos asignados a cada usuario y eliminar accesos innecesarios.

Validación y saneamiento de entradas: Asegurar que todas las entradas del usuario sean validadas y saneadas puede prevenir inyecciones de código y otros ataques similares. Esto implica filtrar caracteres peligrosos y asegurarse de que los datos ingresados cumplan con los formatos esperados.

Implementación de cortafuegos: Utilizar un firewall para aplicaciones web (WAF) puede ayudar a bloquear ataques antes de que lleguen al servidor, proporcionando una primera línea de defensa contra amenazas cibernéticas.

Auditorías y pruebas de seguridad: Realizar auditorías periódicas y pruebas de penetración permiten identificar vulnerabilidades antes de que sean explotadas. Estas pruebas simulan ataques reales para evaluar la seguridad del sistema.

Monitoreo Continuo: Implementar herramientas que escaneen el sitio web en busca de malware y monitoreen la actividad sospechosa puede ayudar a detectar ataques en tiempo real, permitiendo una respuesta rápida a cualquier incidente.

Formación continua del personal: Educar a los empleados sobre las mejores prácticas de seguridad es fundamental. Esto incluye la capacitación sobre cómo reconocer correos electrónicos sospechosos, crear contraseñas seguras y manejar datos confidenciales. Siguiendo estas prácticas, los administradores pueden asegurar que su CMS no solo esté actualizado, sino también protegido contra una amplia gama de amenazas cibernéticas, garantizando así la integridad y disponibilidad del sitio web.

CVE relacionados con vulnerabilidades críticas en versiones desactualizadas de PHP:

Los sistemas de gestión de contenidos (CMS) son vulnerables a diversas amenazas cibernéticas, y algunas de las vulnerabilidades más comunes que afectan a estos sistemas son identificadas por su número CVE (Common Vulnerabilities and Exposures). A continuación, se presentan algunos de los CVEs más críticos y frecuentemente explotados en CMS:

CVE	Descripción	Criticidad CVSS	Año
CVE-2021-26084	Vulnerabilidad en Atlassian Confluence que permite ejecución remota de código.	9.8	2021
CVE-2021-40438	Vulnerabilidad en Apache Struts que permite ejecución remota de código.	9.0	2021
CVE-2017-12635	Vulnerabilidad en Microsoft Dynamics que permite ejecución remota de código.	10.0	2017
CVE-2021-44228	Conocida como "Log4Shell", afecta a Apache Log4j y permite ejecución remota de código.	10.0	2021
CVE-2022-47966	Vulnerabilidad en Oracle WebLogic que permite ejecución remota de código.	9.8	2022
CVE-2019-16759	Afecta a múltiples versiones de software, permitiendo la ejecución remota de código.	9.8	2019
CVE-2020-5902	Afecta a F5 BIG-IP, permitiendo ejecución remota de código sin autenticación.	9.8	2020
CVE-2021-26855	Vulnerabilidad en Microsoft Exchange Server que permite ejecución remota de código.	9.8	2021
CVE-2020-1938	También conocida como GhostCat, afecta a Apache Tomcat y permite acceso no autorizado a archivos.	9.8	2020
CVE-2019-11510	Afecta a múltiples sistemas, permitiendo la ejecución remota de código y comprometiendo datos.	9.8	2019

Fuente: https://cve.mitre.org

Advertencia de Seguridad

Vulnerabilidades comunes de los sistemas de gestión de contenidos (CMS)

COLCERT AD-2009-019

Impacto en Colombia

Aumento de ataques cibernéticos: Las vulnerabilidades en CMS, como las identificadas con CVEs críticos (por ejemplo, CVE-2018-7600 para Drupal), facilitan la explotación por parte de ciberdelincuentes, lo que puede resultar en compromisos significativos de datos y sistemas.

Filtración de datos sensibles: Los CMS a menudo manejan información crítica, incluyendo datos personales y financieros. La explotación de vulnerabilidades puede llevar a la fuga o robo de esta información, lo que no solo afecta a las organizaciones sino también a los usuarios finales, generando desconfianza y potenciales pérdidas económicas.

Desafíos para las pequeñas y medianas empresas (PYMEs): Las PYMEs en Colombia son especialmente vulnerables debido a recursos limitados para invertir en ciberseguridad. La falta de medidas adecuadas para proteger sus CMS puede hacer que sean objetivos fáciles para los atacantes.

Es importante mantener el CMS y sus componentes actualizados, implementar políticas de seguridad robustas y realizar auditorías de seguridad periódicas para proteger el sitio web contra posibles ataques.

NIVEL DE RIESGO

ALTO

FUENTES:

- Common Vulnerabilities and Exposures (CVE) - https://cve.mitre.org/
- National Vulnerability Database (NVD) - Base de datos nacional de vulnerabilidades
- OWASP (Open Web Application Security Project) - Seguridad en aplicaciones web
- CISA (Cybersecurity & Infrastructure Security Agency) - https://www.cisa.gov/
- Drupal - Security advisories - https://www.drupal.org/security
- Joomla - Security Strike Team - https://developer.joomla.org/security.html

COLCERT