GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA

centro nacional de inteligencia
centro criptológico nacional

CCN-CERT
centro criptológico nacional

Hecha pública la Guía CCN-STIC 460 de *Seguridad en Wordpress*

Cómo crear un blog de forma segura con Wordpress

- **La guía proporciona una lista detallada de recomendaciones de seguridad para la configuración de este sistema de gestión de contenidos (CMS[1]) utilizado por cerca del 20% de los sitios web de Internet.**

- **El documento está disponible en la parte pública del portal www.ccn-cert.cni.es, junto con más de 250 documentos de recomendaciones, normas y procedimientos en materia de ciberseguridad.**

Madrid, 27 de julio de 2015.- El Centro Criptológico Nacional (CCN) ha hecho pública su Guía **CCN-STIC 460 Seguridad en Wordpress** con el fin de ofrecer unas recomendaciones de seguridad mínimas a la hora de utilizar este sistema de gestión de contenido (CMS) que, en agosto de 2013, era utilizado por el 18,9% de todos los sitios existentes en Internet, principalmente para la creación de blogs que, por deficiencias de configuración, en muchas ocasiones ha sido utilizado para materializar numerosos ataques

La Guía comienza con un histórico de las distintas versiones que han ido apareciendo de WordPress (creado a partir del desaparecido b2/cafelog) y que debe su éxito, entre otros, a su licencia, su facilidad de uso y sus características como gestor de contenidos.

"Prevención del spam, actualizaciones automáticas, configuración de permisos, copias de seguridad o la recuperación ante un ciberincidente, son algunos de los capítulos de la Guía"

Instalación y actualización, seguridad en la base de datos, procedimiento para la instalación de plugins, bastionado de la cuenta de Administrador, el registro de actividad del sistema o las restricciones de acceso a directorios son algunos de los 22 capítulos que cuenta la Guía.

Además, recoge distintas secciones sobre la prevención de spam, las actualizaciones automáticas, la configuración de permisos, las copias de seguridad o la recuperación ante un compromiso de seguridad.

[1] Content Management System

27 de julio de 2015

Por último, el documento realiza una mención especial a la seguridad personal como el uso de gestores de contraseñas, los antivirus, phishing[2], cortafuegos o seguridad Wi-Fi.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del ENS.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, a sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/
@CCNCERT

https://www.youtube.com/watch?v=5XxS9mZZfKs

[2] Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.