La Guía CCN-STIC 461 puede descargarse de su portal www.ccn-cert.cni.es

El CCN-CERT publica una Guía de Seguridad sobre el gestor de contenidos Drupal

- **El documento recoge las principales prácticas a adoptar para trabajar de forma segura con este CMS (*Content Management System*) libre, utilizado principalmente en el desarrollo y gestión de páginas web.**

- **Histórico de vulnerabilidades, instalación y actualización de Drupal, seguridad en la base de datos, configuración segura de PHP y permisos, restricciones de acceso, instalación de módulos y la creación y recuperación de copias de seguridad son algunos de los capítulos de esta Guía CCN-STIC.**

Madrid, 24 de junio de 2016.- El CCN-CERT ha hecho pública la **Guía CCN-STIC 461 Seguridad en Drupal** que aborda un compendio de buenas prácticas para mantener este CMS de un modo seguro y mitigar los posibles ataques de fuentes externas que puedan tener.

El documento, que puede descargarse de la parte pública del portal del CCN-CERT, expone que se han reportado un total de 290 vulnerabilidades en el período de tiempo comprendido entre 2002 y 2015; y destaca que el 46% de las vulnerabilidades públicas conocidas corresponden a XSS (Cross-Site Scripting).

El documento incluye los siguientes capítulos:

- Introducción
- Instalación y actualización
- Seguridad en la base de datos
- Configuración segura de PHP
- Configuración de permisos
- Creación de un fichero "Robots.txt"
- Restricciones de acceso
- Asegurando el entorno y el usuario #1
- Configuración segura de *Input Formats*
- Administración y navegación sobre SSL
- Administrar Drupal por línea de comandos
- Guía para la instalación de módulos
- Sistema de prueba de módulos y temas

24 de junio de 2016

- Módulos a instalar
- Creación y recuperación de backups
- Recuperación ante un compromiso de seguridad

Guías CCN-STIC

Las **Series CCN-STIC** son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT. El grueso de las Series están especialmente dirigidas al personal de las Administraciones Públicas y empresas y organizaciones de interés estratégico (parte privada del portal) y otras de difusión pública para todos los usuarios. De igual modo, algunas de las series están clasificadas como Difusión Limitada (DL) o Confidencial (C) y por tanto, es necesaria su solicitud al CCN-CERT.

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 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, 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

http://youtu.be/5XxS9mZZfKs

24 de junio de 2016