



Publicada la Guía CCN-STIC 860 de seguridad en el Servicio Outlook Web App (OWA) de Microsoft Exchange Server 2010

Cómo proteger los servicios OWA que permiten el acceso al correo electrónico a través de un servicio web

- La guía se ha elaborado para proporcionar información específica con objeto de realizar una implementación del ENS para el servicio OWA de Microsoft Exchange Server 2010 a través de una configuración de seguridad sólida.
- El documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para la implementación del ENS (CCN-STIC-800) y teniendo como objeto la protección de los servicios prestados a los ciudadanos y entre las diferentes administraciones.

Madrid, 31 de agosto de 2015.- El Centro Criptológico Nacional (CCN) ha hecho pública su **Guía CCN-STIC 860 Seguridad del Servicio OWA en Microsoft Exchange Server 2010**, en donde se ofrece la información y mecanismos para la protección del servicio de Outlook

"Se trata de un servicio altamente expuesto que puede ser atacado para conseguir acceso a la información y a las credenciales con las que acceder a la organización"

Web App (OWA), proporcionado por el servicio de Microsoft Exchange Server y que permite el acceso a los buzones de correo electrónico a través de un servicio web. No obstante estas garantías de acceso, así como la publicación del mismo, constituyen el hecho de que sea un servicio altamente expuesto que puede ser atacado con el objeto no solo de conseguir acceso a la información existente en dicho

servicio, sino como un intento de obtener credenciales con las cuales acceder a la organización.

El documento proporciona una guía de buenas prácticas para la protección de la infraestructura, así como los mecanismos que garanticen el fortalecimiento del servicio OWA. Se incluye además:

- Definición de las condiciones de funcionalidad del servicio de OWA.
- Se referencian los riesgos a los que se enfrenta un servicio Web como OWA.
- Se incorporan mecanismos para la implementación, de forma automática, de las configuraciones de seguridad susceptibles de ello.

31 de agosto de 2015

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es



- Mecanismos de revisión. Se establecen mecanismos de revisión de componentes de OWA para Microsoft Exchange Server 2010.
- Se realiza una presentación de la estructura de ficheros empleados por Microsoft Exchange Server 2010.
- Permite verificar que se cumplen los mecanismos de seguridad definidos en la presente guía.

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para la implementación del Esquema Nacional de Seguridad (CCN-STIC-800) siendo de aplicación para la Administración Pública y teniendo como objeto la protección de los servicios prestados a los ciudadanos y entre las diferentes administraciones.

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/



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

31 de agosto de 2015

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es

