El *Informe de Amenazas CCN-CERT IA-28/15* está publicado en la parte pública del portal

Principales medidas de seguridad en telefonía móvil, nuevo informe del CCN-CERT

- **El documento del CERT Gubernamental Nacional, enfocado tanto para iOS como Android, recoge las medidas más relevantes relacionadas con la pantalla de desbloqueo, las comunicaciones, el software y aplicaciones y el mantenimiento del dispositivo.**

- **El informe recoge un anexo sobre la mitigación de la vulnerabilidad Stagefright, considerada la más crítica en la historia de Android y que afectaba al 95% de estos dispositivos en septiembre de 2015.**

Madrid, 04 de noviembre de 2015. El CCN-CERT, del Centro Criptológico Nacional, ha hecho público su ***Informe de Amenazas IA-28/15 de Medidas de Seguridad en Telefonía Móvil*** en el que recoge un compendio de las medidas de seguridad más relevantes incluidas en sus distintas guías CCN-STIC[1], atendiendo a varios criterios como la seguridad en la pantalla de bloqueo, la seguridad en las comunicaciones y seguridad en el software y aplicaciones. Asimismo, se recogen las principales recomendaciones para el mantenimiento seguro del dispositivo, como la realización de copias de seguridad periódicas o la actualización del *firmware*.

El documento abarca tanto las medidas más relevantes para dispositivos móviles con sistema operativo **iOS**, como para **Android,** incluyendo, además, un anexo sobre cómo mitigar la vulnerabilidad más crítica en la historia de este último sistema operativo: ***Stagefright***. Esta vulnerabilidad afecta a las versiones de Android comprendidas entre la 2.2 y la 5.1.1, lo que representa el 95% de estos dispositivos en septiembre de 2015.

Acceso físico y comunicaciones

Tal y como recoge el informe, es necesario restringir al máximo las acciones que se pueden realizar con acceso físico al teléfono, de modo que únicamente el dueño del mismo sea capaz de usarlo. Por este motivo, se ofrecen diferentes medidas para la pantalla de desbloqueo, como el establecimiento de un PIN para la tarjeta SIM o un código de acceso al dispositivo.

[1] Dentro de la serie 400. CCN-STIC 450-455 (Seguridad en dispositivos móviles, en Android, iPad e iPhone): https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/400-guias-generales.html

Además, los dispositivos móviles cuentan con interfaces de comunicación, tanto físicas (conexión por cable a un ordenador), como por radiofrecuencia (Wifi, 2G/3G/4G, Bluetooth, GPS) y es necesario configurarlos de manera segura para cada una de estas conexiones.

Software y aplicaciones

El potencial de un dispositivo móvil está directamente relacionado con la cantidad y calidad del software que sea posible instalar en el mismo. En este sentido, tanto iOS como Android, poseen una tienda con un número muy alto de aplicaciones (**AppStore y Play Store**), desde donde es posible descargar e instalar un sinfín de programas, que pueden suponer una amenaza contra nuestra privacidad y seguridad.

El Informe recoge también las principales medidas de seguridad a aplicar en este punto.

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