El *Informe de Amenazas IA-05/16* está disponible en la parte pública de su portal web

Informe del CCN-CERT sobre vulnerabilidades en la tecnología NFC

- **El documento aborda los problemas de seguridad en las comunicaciones NFC (*Near Field Communication*) muy utilizadas en aplicaciones cotidianas, como el pago con tarjeta sin contacto, el uso de transporte público o el acceso a edificios controlados.**

- **La escucha secreta o a escondidas, la alteración de la información transmitida y los ataques de retransmisión son los principales problemas encontrados en esta tecnología.**

Madrid, 4 de febrero de 2016.- El CCN-CERT ha hecho público un nuevo Informe de Amenazas **IA-05/16 *Near Field Communication* (NFC) Vulnerabilidades**, en el que se aborda los problemas de seguridad de este tipo de tecnología inalámbrica bidireccional de corto alcance (hasta diez centímetros). Una tecnología que ha despertado gran interés y que tiene multitud de aplicaciones, como identificación de elementos, uso de transporte público, acceso a edificios controlados o pagos bancarios con tarjeta (en el caso de España no se requiere ningún tipo de identificación para cantidades inferiores a 20 euros).

El documento detalla las vulnerabilidades del NFC, mostrando diversos escenarios de ataque como prueba de concepto. Del mismo modo, se resumen las posibles soluciones frente a estos ataques. Cabe recordar que la tecnología NFC está cada vez más presente en los dispositivos móviles, lo que evidencia que más tarde o más temprano empezarán a ser usados como vector de ataque.

En concreto, los problemas de seguridad que sufre NFC son la escucha secreta o a escondidas (*eavesdropping*, en inglés), la alteración de la información transmitida, y los ataques de retransmisión (*relay attacks*). Cabe destacar que las vulnerabilidades destacadas en este informe son inherentes a la propia tecnología NFC, con lo que cualquier sistema que se implemente sobre NFC heredará estos problemas

El Informe puede descargarse desde la parte pública del portal del 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