Boletín informativo del Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PYTEC).

Boletín CCN-PYTEC nº19 - 10/2019

Comunicaciones Tácticas Seguras

Segunda prueba de concepto de LTE seguro desplegable (09/2019).

El 10 de septiembre se llevó a cabo la segunda prueba de concepto de tecnología LTE para entornos desplegables y securizada con soluciones de cifra aprobadas por el CCN para procesar información clasificada. La prueba se llevó a cabo con la celda LTE de la empresa JRC (Japan Radio Co. Ltd.), representada en España por la empresa BlackBull con el apoyo técnico de Galicom Comunicaciones. Sobre esta infraestructura de comunicaciones se empleó con éxito la suite de seguridad conformada por el teléfono móvil rugerizado Bittium Tough Mobile C y la aplicación ComsecAdmin+ de Indra para comunicaciones seguras de voz, datos y video. Tanto el Bittium Tough Mobile C como la app ComsecAdmin+ están incluidas en el Catálogo de Productos STIC en la categoría de Comunicaciones Tácticas Seguras.

La arquitectura de seguridad adoptada en estas pruebas con la celda LTE de JRC es similar a la que se empleó en las pruebas con la celda LTE-TPN400 de la empresa Centum, así como en las pruebas de Wi-Fi seguro llevadas a cabo por la JCISAT del Ejército de Tierra y el CCN.

Productos STIC

La gama Samsung Galaxy S10 obtiene la cualificación de seguridad para sistemas sujetos al ENS (08/2019).

Los dispositivos de la gama Samsung Galaxy S10 se incorporan al listado de Dispositivos Móviles cualificados, considerados aptos para el despliegue en sistemas sujetos al Esquema Nacional de Seguridad. En la guía CCN-STIC 1606 se puede consultar la configuración evaluada y aprobada por el CCN para los dispositivos: Samsung Galaxy S10 / S10e / S10+ / S10 5G, habiéndose comprobado la compatibilidad con los dispositivos previamente cualificados por el CCN.

MobileIron Core, Herramienta de Gestión de dispositivos cualificada por el CCN (08/2019).

El UEM de MobileIron es el primer producto de esta categoría en superar las pruebas de cualificación a nivel nacional tras aportar diferentes certificaciones internacionales (CC, FIPS 140-2, SOC 2…).

La plataforma de Mobileiron ofrece la posibilidad de segurizar cualquier dispositivo que acceda a recursos corporativos desde un despliegue on-premise, dotando a la organización de capacidad de gestión, autonomía y seguridad.

IBM Qradar, cualificado en la familia "Sistemas de gestión de eventos de seguridad" para ENS categoría alta (09/2019).

El producto IBM Qradar se ha incluido en el Catálogo de Productos de Seguridad TIC como cualificado para ENS alto.

QRadar recolecta, consolida y correlaciona información de todos los endpoints, dispositivos de red, entornos de las nubes, aplicaciones e incluso de diferentes data-lakes.

PSTdiode, cualificado y aprobado en la familia "Diodos de datos" (09/2019).

El diodo del fabricante AUTEK ingeniería ha sido incluido en el Catálogo de Productos de Seguridad TIC como cualificado para ENS alto y como aprobado para todos los niveles.

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal es la introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas.

Cisco Firepower Threat Defense (FTD), cualificado para ENS categoría alta (09/2019).

Cisco ha cualificado para ENS categoría alta determinados dispositivos con la versión FTD 6.2 en las familias:

- "Cortafuegos",
- "Redes privadas virtuales: IPSec",
- "Dispositivos de prevención y detección de intrusiones".

Cisco Firepower Threat Defense (FTD) es un appliance, virtual o físico, que tiene las capacidades de firewall, VPN e IPS. Esta plataforma ofrece la capacidad de filtrado de paquetes con estado (stateful packet filtering), y de inspección de paquetes basada en información de las aplicaciones (application-aware). También proporcionan capacidades IPsec para el establecimiento de túneles VPN con otros servidores VPN (VPN peer-to-peer) o con dispositivos VPN cliente (VPN de acceso remoto).

Cortafuegos de Nueva Generación de Fortinet, cualificados para ENS categoría alta (09/2019).

Fortinet ha cualificado para ENS categoría alta determinados dispositivos con la versión FortiOS 5.6 en las familias:

- "Cortafuegos",
- "Redes privadas virtuales: IPSec".

Los dispositivos de FortiGate son cortafuegos de nueva generación con capacidades de inspección en capa 7 y concentrador VPN IPSEC. Dispone de muchos modelos diferentes, desde *appliances* de hardware de nivel básico hasta *appliances* ultra avanzados para cumplir los requisitos más exigentes de rendimiento de protección contra amenazas. Esto garantiza que el campus empresarial, el centro de datos principal o los segmentos internos y FortiGate puedan adaptarse perfectamente al entorno.

authUSB, incluido en el BOA Programme de la Agencia de comunicación e información de la OTAN (09/2019).

authUSB, empresa española de ciberseguridad , presente ya en el catálogo CPSTIC con su solución SafeDoor, ha firmado recientemente un acuerdo con la NATO C&I Agency de la OTAN.

Esto ha hecho posible su entrada en el BOA List, dando a authUSB, como proveedor de SafeDoor, la consideración de Empresa Elegible (Proveedor) de la OTAN.

Actualizada la guía sobre taxonomía de referencia para el Catálogo de Productos de Seguridad TIC (09/2019).

Requisitos fundamentales de seguridad para ENS categoría ALTA

- **Anexo B6 Sistemas de gestión de eventos de seguridad**

Requisitos fundamentales de seguridad paraENS categoría MEDIA

- **Anexo B6.M Sistemas de gestión de eventos de seguridad**
- **Anexo D1.M Enrutadores**
- **Anexo D2.M Switches**

Se ha actualizado la guía CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC en la que se establece una clasificación de productos en torno a diversas categorías y familias como base para la ordenación de los Productos incluidos en el Catálogo de Productos de Seguridad TIC (CPSTIC).

El CPSTIC es un listado de productos STIC de referencia, supervisado por el Centro Criptológico Nacional, CCN, que pretende proporcionar un nivel mínimo de confianza al usuario final, incluyendo los "Productos Aprobados" para manejar información nacional clasificada y los "Productos Cualificados de Seguridad TIC".

A continuación, se destacan los principales cambios que recoge la actualización de la guía CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC:

- Actualización del Anexo B6 Sistemas de gestión de eventos de seguridad, que recoge los requisitos fundamentales de seguridad (RFS) que debe cumplir un producto en un sistema afectado por el **ENS** con categoría **alta**.
- Publicación del **Anexo B6.M Sistemas de gestión de eventos de seguridad**, que recoge los requisitos fundamentales de seguridad (RFS) que debe cumplir un producto en un sistema afectado por el **ENS** con categoría **media**.
- Actualización del Anexo D1.M Enrutadores, que recoge los requisitos fundamentales de seguridad (RFS) que debe cumplir un producto en un sistema afectado por el **ENS** con categoría **media**.
- Publicación del **Anexo D2.M Switches**, que recoge los requisitos fundamentales de seguridad (RFS) que debe cumplir un producto en un sistema afectado por el **ENS** con categoría **media**.

Criptografía

CCN-PYTEC participa como ponente en la jornada de tecnologías cuánticas organizada por la APTIE (09/2019).

El pasado 12 de septiembre el Departamento de Productos y Tecnologías del CCN participó como ponente en la jornada "Tecnologías Cuánticas: Perspectivas y Problemática para la Seguridad de la Información y las Comunicaciones" organizada por la Asociación para la Promoción de las Tecnologías e Industrias Estratégicas (APTIE).

Durante la jornada, se realizaron varias ponencias de investigadores españoles relacionados con las tecnologías cúanticas, la realidad de la amenaza cuántica y la necesidad de comenzar a realizar desarrollos de criptografía postcuántica para poder garantizar la seguridad de las tecnologías de la información frente a la amenza cuántica.

CCN-PYTEC participa en la sesión abierta del proyecto "Comunicación segura en la era cuántica" financiado por el programa de la OTAN "Ciencia por la Paz y la Seguridad" (09/2019).

El 26 de septiembre CCN-PYTEC participó en la sesión abierta del proyecto "Comunicación segura en la era cuántica", que tuvo lugar en el campus de Móstoles de la Universidad Rey Juan Carlos (URJC).

El proyecto *"Secure Communication in Quantum Era"*, financiado por la OTAN a través de su programa SPS (Ciencia para la Paz y la Seguridad), persigue conjugar ambas tecnologías, la clásica y la postcuántica, para conseguir un intercambio de claves entre varios usuarios (en principio, más de dos). "El objetivo es el diseño de esquemas seguros para intercambio de clave en entornos multiusuario, es decir, para el establecimiento de sesiones seguras de comunicación entre distintos actores que sólo pueden comunicarse usando redes inseguras", explica María Isabel González Vasco, co-directora del proyecto.

Los miembros del equipo de investigación ya han comenzado a trabajar en el diseño de un modelo de seguridad, denominado *'quantum-future'*. Esta herramienta se basará en un protocolo de establecimiento de clave que mientras se ejecute no permita el acceso a adversarios cuánticos. "Nuestro objetivo es crear e implementar un esquema (en la medida de lo posible, genérico) de intercambio de clave para varios usuarios resistente a ataques en el modelo *'quantum-future'*.

Dicho esquema podría materializarse a partir de las actuales herramientas disponibles para establecimiento de clave cuántico (el QKD), pero también usando herramientas clásicas post-cuánticas", apunta la investigadora de la URJC.

Interoperabilidad

El CCN participa en el grupo de redacción de la NKMIS (09/2019).

Entre los días 17 y 20 de septiembre el CCN ha participado en La Haya en el grupo de trabajo para la elaboración de la *"Key Management Intoperability Specification"* de OTAN (NKMIS). La elaboración de esta especificación está incluida dentro del programa de trabajo de la NCIA, el cual ha sido promovido por el C3 Board de la OTAN.

El principal objetivo de esta especificación es estandarizar la distribución y gestión de claves para facilitar la interoperabilidad entre equipos cripto y centros de gestión de claves, de forma que una infraestructura común permita dicha gestión independientemente del fabricante del cifrador, e incluso de las naciones que lo estén utilizando. A nivel técnico cabe destacar que esta especificación se basa en el empleo del estándar CMS (*"Cryptographic Message Syntax"*), RFC5652, del IETF (*"Internet Engineering Task Force"*) para la distribución de los distintos tipos de material criptológico.

Contacto

Correo electrónico CCN-PYTEC	**ccn-pytec@cni.es**
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**
Catálogo CPSTIC	**Enlace web**