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

Boletín CCN-PYTEC nº28 - 12/2020

Modernización criptológica

El CCN trabaja en una nueva generación de equipos de cifra (12/2020).

El Centro Criptológico Nacional ha estado trabajando todo este año 2020 en la **modernización criptológica de los equipos nacionales de cifra** para proteger información clasificada. Los esfuerzos se han centrado específicamente en dos ámbitos:

- **Nuevos equipos de cifra en capa 2 (MACsec) y capa 3 (IP)** con nuevas funcionalidades y capacidades (**muy alta velocidad, redundancia**, etc.) adaptadas a las nuevas arquitecturas de red.
- Nuevos algoritmos criptográficos y mecanismos de seguridad que garanticen la **protección de la información frente a la amenaza de la computación cuántica.**

Gestión Electrónica de Claves

Primer prototipo de un cargador de claves nacional, OTAN y UE (12/2020).

La empresa Tecnobit, S.L. (Grupo Oesia) está trabajando en el desarrollo de un **cargador de claves (DTD), denominado ĒRMES,** capaz de operar en dominios de seguridad distintos: **nacional, OTAN y UE**. En función de la "Crypto Ignition Key" (CIK) que se introduce en el dispositivo, el mismo arranca en un modo de operación u otro (nacional, OTAN o UE), permitiendo el acceso a las operaciones de carga y descarga de claves de ese ámbito.

Este mes de diciembre se llevaron a cabo las pruebas de aceptación del expediente del CCN para el desarrollo de un primer prototipo de este cargador de claves. Durante esas pruebas se llevaron a cabo, entre otras, las siguientes pruebas:

- Ámbito OTAN: **descarga de claves de un cargador SKL** ("Simple Key Loader") al cargador ẼRMES, así como transferencia de claves entre cargadores ẼRMES.
- Ámbito UE: **carga de claves** desde ẼRMES **al receptor GALILEO PRS PRESENCE1**.
- Ámbito nacional: **descarga de claves del POC-IS** del Canal Secundario PRS nacional **y carga en un POC-Unidad**.

Además, en las pruebas de fábrica también **se cargaron claves en el módulo de seguridad (SM) del receptor PRS PRESENC2** (ámbito UE), y en un **terminal MIDS-LVT BU1** (ámbito OTAN).

Comunicaciones Tácticas Seguras

El CCN apoya al Ejército de Tierra en las pruebas de aceptación de GESCOMETv4S y la nueva Unidad de Comunicaciones Seguras (12/2020).

Los días 3 y 4 de diciembre CCN-PYTEC apoyo al ET en la ejecución de las **pruebas de aceptación relativas al cifrado de voz y datos por la Red Radio de Combate**, a través de la última versión del Gestor de Comunicaciones de ET (**GESCOMETv4S**) y de la nueva Unidad de Comunicaciones Seguras (**UCS**). Estos dos productos desarrollados por RF Española integran las soluciones de cifra TZ-1001R y TZ-501R (familia CIFPECOM) de Tecnobit.

Estos nuevos productos son **capaces de cifrar varias comunicaciones de voz táctica ("push to talk") y de datos IP de forma simultánea, transmitiendo dicha información a través de los canales habilitados para voz y para datos, respectivamente**, en las diferentes radios de dotación de ET (PR4G, RF5800H, etc.). En el caso particular de la transmisión de **voz táctica cifrada**, esta circunstancia supone una **gran novedad** ya que en los productos de cifra nacional disponibles hasta la fecha, la voz táctica se enviaba encapsulada en datos, lo que solía provocar cortes en la comunicación y el consumo del ancho de banda disponible para las propias comunicaciones de datos. Sin embargo **esta nueva solución transmite la voz táctica cifrada por su canal natural**, aprovechando los mecanismos de priorización habituales de las radios tácticas para la transmisión de voz, y sin consumir el ancho de banda destinado para los datos.

Productos STIC

Publicada la guía CCN-STIC-1502 "Procedimiento de Empleo Seguro para Blancco File Eraser" (11/2020).

El CCN ha publicado la guía CCN-STIC-1502 **"Procedimiento de Empleo Seguro para Blancco File Eraser"**, producto de Blancco Technology Group incluido en la familia de **"Herramientas de borrado seguro"** del CPSTIC. Este procedimiento de empleo seguro se puede consultar en el enlace.

Publicada la guía CCN-STIC-1207 "Procedimiento de Empleo Seguro para Sophos Intercept X Advanced" (12/2020).

El CCN ha publicado la guía CCN-STIC-1207 **"Procedimiento de Empleo Seguro para Sophos Intercept X Advanced"**, producto de Sophos incluido en las familias de **EDR ("Endpoint Detection and Response")** y **EPP ("Endpoint Protection Platform")** del CPSTIC. Este procedimiento de empleo seguro se puede consultar en el enlace.

Contacto

Correo electrónico CCN-PYTEC	**ccn-pytec@cni.es**
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**
Catálogo CPSTIC	**https://ccn.cni.es/cpstic**
Youtube	**youtube.com/channel/UCuSR7guHgx5kgoj6kafOF1Q**

El Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PyTec) promueve el desarrollo, la evaluación, la certificación y el uso de productos para garantizar la seguridad de los sistemas de tecnologías de la información y la comunicación.

CCN-PYTEC
Praeventio sit vincere