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

Boletín CCN-PYTEC nº21 - 12/2019

Novedades en el Catálogo de Productos STIC

SonicWall cualifica sus productos en nuevas familias para ENS categoría ALTA (11/2019)

Cortafuegos

D. prevención y detección de intrusiones

Redes privadas virtuales: IPSec

La versión 6.52 en las series *NSA, SM, TZ* y *SOHOW* de *SonicWall* se han cualificado en las familias de "Dispositivos de prevención y detección de intrusiones" y "Redes privadas virtuales: IPSec" para ENS categoría ALTA. Dichos productos ya formaban parte del CPSTIC en la familia de "Cortafuegos".

La inclusión de estas herramientas en las familias mencionadas garantiza que poseen una certificación funcional que cumple con los requisitos fundamentales de seguridad definidos para cada familia.

Gigamon cualifica nuevos productos en la familia de captura, monitorización y análisis de tráfico para ENS categoría ALTA (11/2019)

Captura, monitorización y Análisis de Tráfico

Las series de productos *GigaVUE* (HD8, HD4, HC3, HC2, HC1) y *GigaVUE* (TA10, TA40, TA100) de la empresa GIGAMON han sido incluidas en el CPSTIC como productos cualificados para ENS categoría ALTA en la familia de "Captura, Monitorización y Análisis de Tráfico".

Dichos productos son agentes de paquetes de red (*Network Packet Brokers*) de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/10g en cobre. Disponen de funcionalidades de filtrado de tráfico L2-3-4-7 con motor de DPI (*Deep Packet Inspection*).

Aruba cualifica y aprueba nuevos productos en varias familias del CPSTIC *(11/2019)*

Enrutadores

Switches

Aruba ha cualificado y aprobado su serie de switches (8320,8325, 8400) Aruba OS-CX con versión 10.03 en las familias de "enrutadores" y "switches" del CPSTIC.

Los *switches* de Aruba están orientados tanto a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos, Además, dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar completamente programable.

La tableta rugerizada Samsung Galaxy Tab Active2 y el dispositivo Samsung Galaxy Note 10, nuevos dispositivos cualificados para ENS categoría ALTA (12/2019).

Los nuevos dispositivos Samsung Galaxy incluidos en el Catálogo de Productos de Seguridad de las TIC permitirán a los organismos de la Administración trabajar en diferentes entornos de movilidad. Se amplía así la gama de productos incluidos en el Catálogo de Productos de Seguridad TIC como cualificados para ENS categoría ALTA en la familia "Dispositivos móviles".

EMSEC

Evaluación TEMPEST de la Fragata F-102 (11/2019).

Durante el mes de noviembre, el laboratorio de Seguridad de Emanaciones y TEMPEST del CCN llevó a cabo la evaluación de la Fragata F-102 "Almirante Juan de Borbón" como parte de la revisión TEMPEST de las distintas plataformas de la Armada que manejan información sensible.

La evaluación se realizó en las instalaciones del Arsenal de Ferrol por parte del personal especialista del laboratorio TEMPEST del CCN en estrecha colaboración con la tripulación de la F-102 conocedora de los detalles técnicos y configuración de los sistemas que eran objeto de evaluación en el buque. La complejidad de la evaluación requirió además la colaboración del CECOM de la Fragata F-101 "Álvaro de Bazán" y del mando de la 31 Escuadrilla de Superficie.

Con motivo de esta evaluación, se aprovechó para impartir formación en cuanto a aspectos de seguridad TEMPEST al personal de la Armada allí destinado, especialmente al personal de Ingeniería, Construcciones y Obras (ICO) implicado en el desarrollo de las futuras F-110.

Comunicaciones Tácticas Seguras

Nuevos modos de voz táctica segura en el cifrador CIFPECOM (12/2019).

A lo largo de este año 2019, gracias a un expediente de I+D de la Subdirección General de Planificación, Tecnología e Innovación (SDGPLATIN) de la DGAM y bajo Dirección Técnica del CCN, la empresa Tecnobit ha implementado nuevos modos de voz táctica segura ("Push-To-Talk") definidos en las nuevas especificaciones criptográficas OTAN para interoperabilidad en este ámbito (STaC-IS y TSVCIS). Estos nuevos modos de voz segura han sido implementados en el Cifrador Personal del Combatiente (CIFPECOM) y proporcionan un abanico de soluciones de cifrado que puedan ser usadas con diversos tipos de radios (HF, VHF, etc.), especialmente en aquellos casos en los que el canal es más hostil.

El resultado de este proyecto podrá ser incorporado en un futuro próximo como solución de cifrado para el Gestor de Comunicaciones del Ejército de Tierra (GESCOMET), así como servir de base para otras soluciones de cifra para la Red Radio de Combate.

Sistemas de Navegación Segura por Satélite

Objetivos nacionales para el año 2020 en Galileo PRS (12/2019).

El año 2020 se presenta lleno de desafíos para la implantanción nacional de los servicios para navegación segura por satélite de "*Galileo Public Regulated Service*" (Galileo PRS).

El CCN está involucrado en estas actividades ya que los productos PRS cuentan con módulos de seguridad que han de someterse a un proceso de aprobación para Unión Europea y, por otra parte, porque los sistemas de gestión asociados a los receptores manejan información clasificada.

A lo largo de 2020, se prevé la finalización del desarrollo del primer receptor PRS nacional cuyo módulo de seguridad va a ser sometido inicialmente a un proceso de evaluación nacional por parte del CCN, y posteriormente a una "*Second Party Evalution*" (SPE) por parte de una nación AQUA para la aprobación UE. Este receptor, denonimado **PRESENCE2**, está siendo desarrollado por las empresas GMV y Tecnobit y se espera que pueda ser desplegado en el vehículo de combate a ruedas VCR 8x8 y en las fragatas F-110 como parte de su sistema de navegación.

Además, está previstá la puesta en marcha del proyecto europeo **GEODE** dentro del cual España trabajará para la consecución de receptores PRS de un factor de forma menor.

Por otra parte, el CCN seguirá apoyando técnicamente al INTA en sus funciones como CPA española (Autoridad Competente en PRS), en la implatanción de una infraestructura de **Canal Secundario Nacional** para Galileo PRS. Esta infraestructura, compuesta por una serie de nodos jerárquicos conocidos como POCs, ofrecerá la posibilidad de complementar y mejorar la señal primaria procedente de los satélites (p.ej. optimización de los tiempos de envío de mensajes a los receptores), gestionar los receptores PRS nacionales (enviándoles órdenes específicas, "*re-key*" por el aire, envío de mensajes de anulación del servicio a receptores perdidos, etc.) sin necesidad de que se realice a través del GSMC y otros centros de control de Galileo. Además, este Canal Secundario permitirá a los receptores nacionales contar con un canal de retorno de datos (p.ej. posición, velocidad y tiempo - *PVT*) hacia la jerarquía de POCs de los que depende.

En 2020 está previsto que el POC-IS (nodo principal de la jerarquía), ubicado en el INTA, sea acreditado junto con la interconexión con nodos de menor nivel para actividades de experimentación; con ello se pretende que el sistema alcance una capacidad operativa inicial.

Finalmente, también continuarán las actividades de desarrollo de un **cargador de claves (KFD) dual** que pueda servir tanto para los receptores PRS (ámbito UE) como para los diferentes elementos que componen el Canal Secundario (ámbito nacional).

Eventos

Éxito del módulo sobre Prevención en Ciberseguridad y Soluciones Tecnológicas durante las XIII Jornadas STIC CCN-CERT (12/2019).

Las XIII Jornadas STIC CCN-CERT, celebradas en Madrid durante los días 10, 11 y 12 de diciembre, contaron con la asistencia record de más de 3.300 personas. En esta edición, bajo el lema "**Comunidad y Confianza, bases de nuestra ciberseguridad**", participaron 130 ponentes de reconocido prestigio distribuidos entre 7 módulos con temática diferente. Además, durante el día 10 de diciembre se llevaron a cabo 16 talleres prácticos, destacando el taller "*Färist Mobile: combining strong security with usability*", relativo a comunicaciones móviles seguras.

El Departamento de Productos y Tecnologías del CCN dirigió el Módulo 3 sobre Prevención en Ciberseguridad y Soluciones Tecnológicas. De este módulo cabría destacar, entre otras, la ponencia "***Cybersecurity Act***", impartida por CCN-PYTEC; "La amenaza cuántica, ¿hay cripto después?", impartida por el Centro Superior de Investigaciones Científicas; o la ponencia "Comunicaciones móviles para gestión de crisis", impartida por la empresa Bittium. Todas las ponencias suscitaron gran interés y generaron un gran número de preguntas. Además, las referencias a la necesidad y utilidad del Catálogo de Productos STIC del CCN para la Administración fueron una constante en todas las presentaciones.

CCN-PYTEC volverá a estar presente en la XIV edición de la Jornadas para continuar dando respuesta a las inquietudes trasladadas por la Administración y empresas.

Contacto

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


2020
ENS
Seguridad
EVALUACIÓN
CPSTIC
OC
Cripto
ENECSTI
Cualificación
Common Criteria
CCN-PYTEC
FELIZ NAVIDAD
LINCE
Desarrollo STIC
CIFRA
TEMPEST
EMSEC
@
Certificación


El Centro Criptológico Nacional
les desea Feliz Navidad y un
próspero Año 2020
CCN
centro criptológico nacional