Boletín informativo del departamento de productos y tecnologías de seguridad TIC del Centro Criptológico Nacional (CCN-PYTEC).

Boletín CCN-PYTEC nº23 - 04/2020

Novedades en el Catálogo de Productos STIC

Actualizada la guía sobre taxonomía de referencia para el Catálogo de Productos de Seguridad TIC (04/2020).

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:

- Dentro de la categoría "Protección de Equipos y Servicios", se crea la familia "CASB" (*Cloud Access Security Broker*). Los productos CASB (Cloud Access Security Broker) dan respuesta a la necesidad de visibilidad y control sobre el uso que hacen los usuarios de una organización de las aplicaciones y servicios en la nube. Representan un punto central en el que la organización puede implementar políticas de seguridad que regulen el uso que realizan usuarios y dispositivos, de aplicaciones y servicios en la nube. Los requisitos fundamentales de seguridad (RFS) de esta familia se recogen en el Anexo F.9.
- También dentro de la categoría "Protección de Equipos y Servicios", se crea una nueva familia de "Hiperconvergencia". La infraestructura hiperconvergente (HCI) es un enfoque de arquitectura basada en software, que proporciona recursos de almacenamiento, cómputo y redes de forma transparente al hardware que se utilice, con grandes capacidades de escalado horizontal y todo ello gestionado desde un único punto centralizado. Los productos asociados a esta familia integran las capacidades de cómputo, de almacenamiento y de red en una misma capa de funcionamiento, centralizando todas las tareas de gestión propias de los centros de datos, a nivel software. Los RFS aplicables a esta familia se recogen en el Anexo F.10.
- Se crea una nueva familia de "Servicios en la Nube". La adopción de servicios en la nube como estrategia para soportar los servicios TIC ofrecidos por distintos organismos presenta un amplio

número de ventajas. Sin embargo, este nuevo paradigma tecnológico introduce nuevos riesgos que deben controlarse para poder prestar un servicio que garantice la seguridad de los activos sensibles del organismo que maneje el servicio en la nube, así como el cumplimiento de los requisitos exigidos por los marcos legales de aplicación. Estos riesgos añadidos con respecto a los de un producto *on-premise* afectan a la confidencialidad, integridad, disponibilidad y trazabilidad de la información y por lo tanto, deben ser analizados y gestionados mediante la aplicación de medidas y procedimientos de seguridad. Los RFS aplicables a la familia de "Servicios en la Nube" se recogen en el Anexo G. Dichos requisitos son aplicables a cualquier servicio de seguridad en la nube y deben ser entendidos como requisitos adicionales que complementan a los requisitos definidos para cada una de las familias de productos incluidas en la taxonomía detallada en la presente guía.

Citrix Systems cualifica su producto Citrix ADC en la familia "Control de Acceso a Red" para ENS categoría ALTA (04/2020).

Citrix ADC (antes NetScaler) es un "Application Delivery Controller" con funciones específicas de seguridad para el control de acceso a la red corporativa de usuarios y dispositivos, permitiendo discriminar en el acceso no solo por usuario sino también por el estado de la seguridad en el momento de la conexión y durante la misma. Tanto en accesos SSL VPN como mediante un portal completo de aplicaciones servido al usuario -donde están sus aplicaciones internas, SaaS y aplicaciones y desktops virtuales-, se autenticará al usuario (con opción de múltiples factores, incluso con OTP Nativo sin necesidad de otro OTP adicional) contra un sistema corporativo o mediante federación de identidades, se tendrá en cuenta su perfil (usuario, grupos, atributos en el Directorio), y se comprobará la seguridad del dispositivo (antivirus, firewall, dominio, procesos activos, etc.) y la de la conexión (punto de acceso, ubicación desde la que se accede, etc.), para aplicar según el resultado unas políticas de acceso granulares, ya sea en el propio appliance o en un dispositivo de red posterior como un firewall. De esta forma se garantiza el acceso a cada recurso interno únicamente de aquellas combinaciones aprobadas de usuario/dispositivo/conexión.

Forescout cualifica su producto Forescout 8.1 en la familia "Control de Acceso a Red" para ENS categoría ALTA (04/2020).

La plataforma Forescout es una plataforma unificada de seguridad que permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Se despliega de forma rápida y segura en entornos de campus, centros de datos, la nube y redes de OT. Ofrece descubrimiento, clasificación en tiempo real y evaluación continua de estado, sin necesidad de agentes. Para más información, visite la web del fabricante.

ESET cualifica su producto ESET Endpoint Security en la familia "Anti-virus / Endpoint Protection Platform" para ENS categoría MEDIA (04/2020).

ESET Endpoint Security es una solución fácil de implementar y utilizar, administrable de forma centralizada, con protección multicapa que se basa en tres pilares básicos: primar el rendimiento del sistema, una detección eficaz y no importunar al usuario con falsos positivos. Este enfoque de protección multicapa permite a ESET detectar y/o bloquear diferentes tipos de amenazas, como ransomware, ataques sin archivos, botnets, ataques de red o exploits.

Entre las tecnologías con detección multicapa que utiliza se encuentra:

- Análisis UEFI: comprueba y aplica la seguridad del entorno previamente al inicio del sistema operativo.
- Detecciones ADN: permite detectar código dañino modificado o cifrado mediante la detección de su comportamiento.
- "Machine Learning": ofrece una mejora de las tasas de detección y un menor número de falsos positivos mediante el propio motor interno de aprendizaje automático.
- Sistema de protección de malware en la nube: permite asilar de forma automática las muestras recopiladas y analizar su comportamiento, recibiendo todos los usuarios de ESET las detecciones sin necesidad de esperar a la próxima actualización del motor de detección.

McAfee cualifica su producto "McAfee Data Loss Prevention (DLP) Endpoint with ePolicy Orchestrator 5.10" en la familia "Sistemas para prevención de fugas de datos" para ENS categoría ALTA (04/2020).

McAfee DLP Endpoint proporciona protección integral para todos los posibles canales de fuga de datos, como dispositivos de almacenamiento extraíbles, la nube, correo electrónico, la mensajería instantánea, la Web, el material impreso, el portapapeles, capturas de pantalla, las aplicaciones para compartir archivos, etc. Sus principales características son:

- Integración con análisis de comportamientos de usuarios (UEBA) de terceros.
- Clasificación manual.
- Análisis y reparaciones iniciados por el usuario.
- Clasificación flexible, que ofrece diccionarios, expresiones regulares y algoritmos de validación.
- Una exclusiva tecnología de etiquetado para identificar los documentos según su origen, que impide que la información confidencial de las aplicaciones web, las aplicaciones de red y los recursos compartidos de red se duplique, renombre o salga de las instalaciones de la empresa.
- Compatibilidad con virtualización para proteger equipos de sobremesa remotos y soluciones VDI.

MIL2004-2xHSR-L3 del fabricante SoCe System-on-Chip engineering – Novatronics, producto aprobado dentro de las familias "Enrutadores" y "Switches" (04/2020).

Router/Switch gestionado, rugerizado de alta disponibilidad, con 20 puertos cobre 1Gb y 4 puertos fibra hasta 10 GbE. Se trata de un COTS potente, abierto y flexible con capacidades "Edge-Computing" gracias a sus procesadores multicore CPU, GPU y FPGA Ultrascale. Su arquitectura reconfigurable permite tecnologías HSR y PRP para asegurar el 100% de la transmisión de datos sin interrupciones ni retrasos en la entrega de paquetes incluso cuando hay fallos de red. Cuenta con TSN para una interoperabilidad con ancho de banda garantizado y latencia determinista, sincronización IEEE 1588 v2 PTP y el máximo nivel de seguridad ante ciberataques y otras amenazas. Certificado MIL-STD-461G y MIL-STD-810G, entre otros, está equipado con sistemas electrónicos auxiliares activos y de supervisión, indispensables para los programas de próxima generación, proporcionando una mayor seguridad de la carga útil, un mayor control del sistema y una fácil integración. El chasis cuenta con filtros EMI/EMC, protección de voltajes y temperaturas extremos.

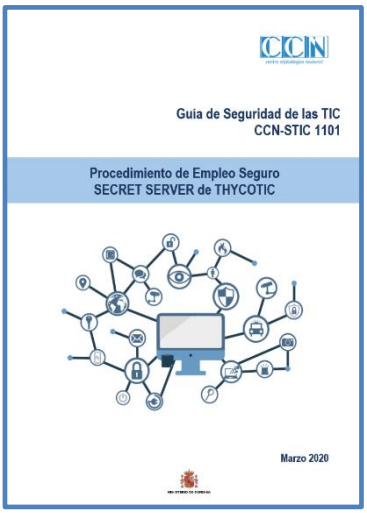
Publicada la Guía CCN-STIC-1101 Procedimiento de empleo seguro SECRET SERVER de THYCOTIC (03/2020).

Se ha publicado el procedimiento de empleo seguro del Secret Sever Government Edition. El producto Secret Sever Government Edition de la empresa Thycotic ha sido cualificado para ENS categoría Alta dentro de la familia: Gestión de acceso privilegiado (PAM)

Thycotic Secret Server es una solución de gestión de cuentas privilegiadas que permite descubrir, securizar, administrar y auditar contraseñas, credenciales así como monitorizar y grabar las sesiones privilegiadas.

Las capacidades de PAM de Secret Server para la administración de las cuentas privilegiadas incluyen:

- Gestión del Ciclo de Vidade las credenciales con privilegios:
  - Descubrimiento automatizado de cuentas privilegiadas y "onboarding" de las mismas en un Repositorio central seguro
  - Rotado automático de las credenciales y Gestión, control y auditoria de las sesiones privilegiadas Análisis del comportamiento del usuario privilegiado
- Gestión de cuentas de servicio
- Políticas de acceso basadas en RBAC y Gestión de políticas de seguridad.
- Arquitectura escalable. Alta Disponibilidad y DR. Integración con múltiples plataformas Out-Of-The-Box
- Módulo de Reporting capaz de generar informes totalmente a medida
- Securización de los procesos de DevOps.



Desarrollo y evaluación de productos cripto

Proyecto para contar con una librería cripto nacional de referencia (04/2020).

El CCN va a inciar un proyecto para contar con una librería cripto de referencia, que sea de utilidad tanto para los laboratorios pertenencientes al Esquema Nacional de Evaluación y Certificación STIC (ENECSTIC) como para los fabricantes de productos de seguridad. El proyecto partirá de una librería cripto "open source" contrastada, la cual será revisada y sanitizada para únicamente incluir las primitivas cripto aceptadas en el documento "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms". Además, sobre esa librería, que previamente ya ha sido evaluada por la Autoridad de Certificación Criptológica de otro país, se llevarán a cabo pruebas adicionales en línea con lo especificado en el "Harmonised Cryptographic Evaluation Procedures" de SOG-IS. Dichas pruebas permitirán verificar nacionalmente la robustez de las primitivas criptográficas seleccionadas. El resultado de este proyecto estará a disposición de los laboratorios del ENECSTIC, para que puedan emplear esa librererría cripto del CCN durante las evaluaciones funcionales de seguridad que lleven a cabo (Common Criteria o LINCE). Además, la librería también estará a disposición de los fabricantes para su uso durante el desarrollo de productos STIC.

EMSEC

Actualización de la guía CCN-STIC-104 (03/2019).

En marzo se ha publicado una nueva versión actualizada de la guía CCN-STIC-104 "Catálogo de Productos con clasificación ZONING" que incluye los últimos equipos y sistemas evaluados por el laboratorio TEMPEST del CCN. La consulta de este catálogo permite obtener una orientación en cuanto a la selección de equipamiento informático que pueda cumplir con una determinada clasificación ZONING.

Es de aplicación para equipos que manejen información clasificada NATO CONFIDENTIAL/EU CONFIDENTIAL/CONFIDENCIAL, o superior, y vayan a ser instalados en locales con clasificación ZONING de ZONA 1 o superior. La clasificación mostrada en esta guía es sólo orientativa y no exime de la necesidad de evaluar los equipos, especialmente si la información que se va a procesar es NATO SECRET/EU SECRET/ RESERVADO o superior.

Contacto

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