Del 5 al 18 de mayo

AVISOS SCI

EUSKO JAURLARITZA
GOBIERNO VASCO

EKONOMIAREN GARAPEN, JASANGARRITASUN ETA INGURUMEN SAILA

DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIDAD Y MEDIO AMBIENTE

GRUPO spri TALDEA

Basque CyberSecurity Centre

Ataque MitM en productos Anybus de HMS Networks

El investigador Ingo Suleck de WAGO ha reportado al fabricante una vulnerabilidad, de severidad alta, que afecta a productos Anybus, cuya explotación podría permitir la realización de un ataque MitM (Man-in-the-Middle).

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en productos ADS-TEC

La empresa afectada ADS-TEC, coordinada por el CERT@VDE, ha identificado múltiples vulnerabilidades en distintos productos, concretamente 8 críticas, 9 altas y 1 media.

Avisos SCI - Del 5 al 18 de mayo

Transmisión de información confidencial sin cifrar en productos de Schneider Electric

Schneider Electric ha comunicado que existe una vulnerabilidad de severidad alta que podría provocar la divulgación de información confidencial sin cifrar, la denegación de servicio o la modificación de datos si un atacante es capaz de interceptar el tráfico de red.

Avisos SCI - Del 5 al 18 de mayo

Avisos de seguridad de Siemens de mayo de 2023

Siemens ha publicado en su comunicado mensual varias actualizaciones de seguridad de diferentes productos.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en Modular Switchgear Monitoring (MSM) de Hitachi Energy

Hitachi Energy ha reportado 2 vulnerabilidades críticas y 6 vulnerabilidades de severidad alta, cuya explotación podría permitir a un atacante obtener credenciales de acceso de usuario de la interfaz web de MSM, así como causar una condición de denegación de servicio.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en Weston Embedded uC-FTPs

Kelly Leuschner, investigadora de Cisco Talos, ha reportado 3 vulnerabilidades, 1 de severidad alta y 2 de severidad media, que afectan al RTOS uC-FTPs de uC-FTPs, y cuya explotación podría permitir a un atacante omitir el proceso de autenticación o causar una condición de denegación de servicio (DoS).

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en productos Teltonika

El investigador, Roni Gavrilov, de Otorio y Claroty Team82, ha reportado 8 vulnerabilidades que afectan a múltiples productos de Teltonika: 3 de severidad crítica, 4 altas y 1 media, cuya explotación podría exponer información sensible del dispositivo y credenciales del mismo, permitir la ejecución remota de código, exponer dispositivos conectados administrados en la red y permitir la suplantación de dispositivos legítimos.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en PTC Vuforia Studio

El Red Team de la compañía aeroespacial Lockheed Martin ha reportado 6 vulnerabilidades en el producto Vuforia Studio de PTC: 1 de severidad alta, 3 medias y 2 bajas. La explotación de estas vulnerabilidades podría permitir a un atacante visualizar credenciales, realizar un CSRF, reenviar peticiones o subir o borrar archivos arbitrarios.

Avisos SCI - Del 5 al 18 de mayo

Inyección SQL en PnPSCADA de SDG Technologies

Momen Eldawakhly, de Samurai Digital Security Ltd, ha informado de una vulnerabilidad de severidad crítica que podría permitir a un atacante interactuar con la base de datos y recuperar datos críticos.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en AirVantage Platform de Sierra Wireless

Roni Gavrilov, de Otorio, ha reportado dos vulnerabilidades, una de severidad alta y una de severidad media, que podrían permitir a un atacante modificar la configuración de los dispositivos, así como recibir información sensible de los mismos.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en productos de BirdDog

Alan Cao ha reportado dos vulnerabilidades de severidad alta, que podrían permitir a un atacante ejecutar código de forma remota u obtener acceso no autorizado.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en productos MB Connect Line

La empresa Helmholz y el investigador Hussein Alsharafi han reportado 2 vulnerabilidades, 1 de severidad media y 1 alta, respectivamente, que afectan a productos de MB Connect Line. A su vez, CERT@VDE se ha coordinado con MB Connect Line y Helmholz para la publicación de las mismas.

Avisos SCI - Del 5 al 18 de mayo

Consumo no controlado de recursos en OPC UA de OPC Foundation

El equipo de investigación de Claroty "Team82", en colaboración con Trend Micro Zero Day Initiative, han reportado una vulnerabilidad de severidad alta, que podría permitir a un atacante bloquear aplicaciones de servidor OPC UA.

Avisos SCI - Del 5 al 18 de mayo

Inyección de comandos sobre el sistema operativo en múltiples productos de WAGO

Quentin Kaiser de ONEKEY ha reportado, en colaboración con CERT@VDE, una vulnerabilidad de severidad crítica. La explotación de esta vulnerabilidad podría permitir a un atacante provocar comportamientos no deseados en los dispositivos afectados, así como causar condiciones de denegación de servicio o un compromiso total del sistema.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en OvrC Pro de Snap One

Uri Katz de Claroty ha informado de que existen 8 vulnerabilidades: 7 de severidad alta y 1 de severidad media, que podrían permitir que un atacante suplante y reclame dispositivos, ejecute código arbitrario y divulgue información sobre el dispositivo afectado.

Avisos SCI - Del 5 al 18 de mayo

Múltiples vulnerabilidades en Terra AC wallbox de ABB

Los investigadores Andi Leach, Puck Meerburg y Lionel R. Saposnik han reportado 2 vulnerabilidades de severidad alta en Terra AC wallbox, cuya explotación podría permitir a un atacante utilizar el producto y modificar o leer los ajustes de configuración del mismo, así como monitorizar la transmisión de datos si está cerca mientras un usuario legítimo utiliza el nodo del sistema.

Avisos SCI - Del 5 al 18 de mayo

Omisión de autenticación en MELSEC WS Series de Mitsubishi Electric

Mitsubishi Electric ha publicado una vulnerabilidad de severidad alta que podría facilitar a un atacante conectarse a través de Telnet y realizar acciones indebidas, manipular la configuración del módulo, o reescribir la firma.

Avisos SCI - Del 5 al 18 de mayo