Del 13 al 25 de enero

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

Múltiples vulnerabilidades en Sewio RTLS Studio

Andrea Palanca, de Nozomi Networks, ha reportado 9 vulnerabilidades que afectan a RTLS Studio, 4 de severidad crítica, 2 altas y 3 medias. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante obtener acceso no autorizado al servidor, alterar información, crear una condición de denegación de servicio (DoS), escalar privilegios y ejecutar código arbitrario.

Avisos SCI - Del 13 al 25 de enero

Múltiples vulnerabilidades en SAUTER Controls Nova

Jairo Alonso Ortiz, Aarón Flecha Menéndez e Iñaki Lázaro Ayanz, investigadores de S21Sec, han notificado 2 vulnerabilidades en SAUTER Controls Nova, 1 de severidad crítica y 1 alta, cuya explotación podría permitir la visualización de información sensible no autorizada y la ejecución remota de código.

Avisos SCI - Del 13 al 25 de enero

Múltiples vulnerabilidades en RONDS EPM

TsungShu Chiu, de CHT Security, ha reportado 2 vulnerabilidades de severidad alta, cuya explotación podría permitir a un atacante no autorizado filtrar las credenciales de inicio de sesión, así como descargar archivos. En algunos casos, el atacante, no autorizado, podría hacer uso de las credenciales de inicio de sesión obtenidas para llevar a cabo una ejecución remota de código.

Avisos SCI - Del 13 al 25 de enero

Múltiples vulnerabilidades en productos InHand Networks

Roni Gavrilov, de OTORIO, ha reportado 5 vulnerabilidades que afecta a InRouter302 e InRouter615: 1 de severidad crítica, 2 altas y 2 medias. La explotación exitosa de estas vulnerabilidades podría permitir la divulgación de información confidencial en texto sin cifrar, la inyección de comandos del sistema operativo, el uso de un hash unidireccional con un salt predecible, el control de acceso inadecuado y el uso de valores insuficientemente aleatorios.

Avisos SCI - Del 13 al 25 de enero

Cross-Site Request Forgery en productos Panasonic

Gjoko Krstic, de Zero Science Lab, ha reportado una vulnerabilidad que afecta a cámaras de red CCTV Sanyo. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante realizar cambios con privilegios de administrador.

Avisos SCI - Del 13 al 25 de enero

Credenciales en texto plano en productos de Johnson Controls

Johnson Controls, Inc. ha reportado una vulnerabilidad de severidad alta, cuya explotación podría permitir a un atacante no autorizado obtener las credenciales en plano.

Avisos SCI - Del 13 al 25 de enero

Vulnerabilidad en productos de HIMA

CERT@VDE, coordinado con HIMA, ha publicado un aviso que contiene 1 vulnerabilidad de severidad alta. La explotación de esta vulnerabilidad podría permitir al atacante obtener privilegios y acceso completo al sistema.

Avisos SCI - Del 13 al 25 de enero

Divulgación de información sensible en productos de Campbell Scientific

INCIBE ha coordinado la publicación de 1 vulnerabilidad en los dataloggers mencionados de Campbell Scientific, que ha sido descubierta por Carlos Antonini Cepeda.

A esta vulnerabilidad se le ha asignado el código CVE-2023-0321. Se ha calculado una puntuación base CVSS v3.1 de 9,1, siendo el cálculo del CVSS el siguiente:
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Avisos SCI - Del 13 al 25 de enero

Múltiples vulnerabilidades en Proficy Historian de GE Digital

Uri Katz, de Claroty Research, ha reportado 4 vulnerabilidades de severidad alta, y una vulnerabilidad de severidad crítica, cuya explotación podría permitir el bloqueo del dispositivo después del acceso, causando un desbordamiento de búfer y pudiendo permitir una ejecución remota de código.

Avisos SCI - Del 13 al 25 de enero

Vulnerabilidad de denegación de servicio en Hitachi Energy PCU400

Hitachi Energy ha informado de dos vulnerabilidades en la versión de la liberaría OpenSSL incluida en los sistemas, que podría causar una condición de denegación de servicio, tanto en la función de registro del dispositivo, como en su servidor asociado.

Múltiples vulnerabilidades en XINJE XD

Mashav Sapir, de Claroty, ha notificado dos vulnerabilidades de severidad alta en la programación de XINJE XD, que podrían permitir a un atacante escribir en archivos de proyectos arbitrarios de un PLC y obtener privilegios de ejecución.

Múltiples vulnerabilidades en LANTIME de Meinberg

Meinberg ha publicado nuevas versiones de su firmware LANTIME que incluyen actualizaciones de seguridad de varias bibliotecas y programas de terceros.

Avisos SCI - Del 13 al 25 de enero