Febrero 2022

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 productos Gerbv

Claudio Bozzato, de Cisco Talos, ha descubierto 2 vulnerabilidades en productos de Gerbv: 1 de severidad crítica y 1 media, que podrían permitir a un atacante realizar una ejecución de código y divulgación de información.

Vulnerabilidad en WIBU-SYSTEMS Codemeter

WAGO, en coordinación con CERT@VDE, ha publicado una vulnerabilidad en WIBU-SYSTEMS Codemeter. Todos los paquetes de instalación de e!COCKPIT y WAGO-I/O-Pro (CODESYS 2.3) existentes actualmente están afectados con versiones vulnerables.

Avisos SCI - Febrero 2022

Inyección de comandos en Industrial Cellular Router de Ricon Mobile

Gjoko Krstic, de Zero Science Lab, ha reportado al CISA una vulnerabilidad de severidad crítica por la que un atacante podría inyectar y ejecutar comandos shell arbitrarios como administrador.

Avisos SCI - Febrero 2022

Clave criptográfica embebida en productos Advantech

La existencia de claves criptográficas embebidas podría permitir a un atacante el acceso no autorizado en el servidor web para interceptar el tráfico.

Avisos SCI - Febrero 2022

Múltiples vulnerabilidades en productos Sealevel Systems

Francesco Benvenuto y Matt Wiseman, de Cisco Talos, han reportado 10 vulnerabilidades: 4 críticas, 6 altas y 3 bajas, que podrían permitir a un atacante controlar las funcionalidades del dispositivo, la sobreescritura arbitraria de archivos, la ejecución remota de código, la escritura fuera de límites, la divulgación de información o la denegación del servicio.

Múltiples vulnerabilidades en Sante DICOM Viewer Pro

Tran Van Khang (khangkito) de VinCSS, y Mat Powell de Trend Micro ZDI, han notificado 7 vulnerabilidades de severidad alta que afectan a DICOM Viewer Pro de Sante. Estas vulnerabilidades podrían permitir a un atacante remoto ejecutar código arbitrario en caso de que el usuario visite una web maliciosa o abra un archivo infectado.

Avisos SCI - Febrero 2022

Múltiples vulnerabilidades en Airspan Networks Mimosa

Noam Moshe, investigador de Claroty, ha reportado 7 vulnerabilidades en Mimosa de Airspan Networks: 4 con severidad crítica, 2 altas y 1 media, que podrían permitir a un atacante obtener información sensible del usuario, ejecutar código remoto no autorizado en todos los dispositivos Mimosa conectados a la nube y comprometer la instancia EC2 en la nube de AWS y buckets S3.

Validación inadecuada de los datos de entrada en Sensormatic PowerManage

La validación inadecuada de los datos de entrada podría permitir a un atacante la ejecución remota de código.

Avisos SCI - Febrero 2022

Múltiples vulnerabilidades en productos de Schneider Electric

Schneider Electric ha publicado 20 vulnerabilidades, siendo 5 de severidad crítica, 8 altas y 7 medias.

Avisos SCI - Febrero 2022

Avisos de seguridad de Siemens de febrero de 2022

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

Avisos SCI - Febrero 2022

Denegación de servicio en productos ABB

Múltiples vulnerabilidades podrían permitir a un atacante con acceso a la red de control del sitio, la denegación del servicio.

Avisos SCI - Febrero 2022

Múltiples vulnerabilidades en productos Moxa

Moxa ha notificado 3 vulnerabilidades del tipo uso de credenciales embedidas en texto claro y transmisión de información sensible sin cifrar.

Avisos SCI - Febrero 2022

Fin de soporte en ventiladores Dräger

DrÃ¤ger ha reportado una vulnerabilidad por la que un atacante podría comprometer a la seguridad y eficacia de los dispositivos afectados.

Avisos SCI - Febrero 2022

Vulnerabilidades INFRA:HALT en productos Eaton

Eaton ha publicado un aviso, detallando que varios productos se ven afectados por vulnerabilidades en la pila de InterNiche, cuya explotación podría permitir a un atacante tomar el control del sistema afectado.

Avisos SCI - Febrero 2022

Múltiples vulnerabilidades en AVEVA System Platform

Sharon Brizinov, de Claroty, junto con Ilya Karpov, Evgeniy Druzhinin y Konstantin Kondratev, de Rostelecom-Solar, coordinados por el ICS-CERT, han notificado vulnerabilidades en AVEVA System Platform.

Avisos SCI - Febrero 2022

Múltiples vulnerabilidades en Energy Saving Data Collecting Server de Mitsubishi Electric

Mitubishi Electric ha notificado 9 vulnerabilidades, 2 de severidad alta y 7 de severidad media por las que permitiría a un atacante la divulgación de información o la manipulación del producto.

Avisos SCI - Febrero 2022

Ejecución remota de código en LeviStudioU de WECON

Natnael Samson, de Zero Day Initiative, ha reportado 2 vulnerabilidades de severidad alta que podrían permitir a un atacante la ejecución remota de código en LeviStudioU.

Avisos SCI - Febrero 2022

Divulgación de información en Texas Instruments CC3200 SimpleLink

Francesco Benvenuto y Matt Wiseman, investigadores de Cisco Talos, han identificado una vulnerabilidad de severidad media que podría permitir la divulgación de información.

Avisos SCI - Febrero 2022

Múltiples vulnerabilidades en Simcenter Femap de Siemens

Zero Day Initiative de Trend Micro ha coordinado la publicación, junto con el fabricante Siemens, de 2 vulnerabilidades de severidad alta que podrían explotarse para filtrar información o realizar una ejecución remota de código (RCE).

Avisos SCI - Febrero 2022