

Hasta el 8 de marzo

# AVISOS SCI



# Múltiples vulnerabilidades en EIP Stack Group OpENer

---

Cisco Talos ha descubierto 3 vulnerabilidades, dos de severidad crítica y una de severidad alta, en EIP Stack Group OpENer, una pila de Ethernet/IP para dispositivos adaptadores de E/S, que podría permitir a un atacante provocar que un servidor objetivo se bloquee o abra la puerta a la ejecución remota de código.

Avisos SCI - Hasta el 8 de marzo

# Vulnerabilidad XSS en GigaVue-FM

---

NCIBE ha coordinado la publicación de 1 vulnerabilidad en GigaVUE-FM de Gigamon, que ha sido descubierta por Albert Sanchez Miñano.

A esta vulnerabilidad se le ha asignado el código CVE-2023-0746. Se ha calculado una puntuación base CVSS v3.1 de 6,3, siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L.

Avisos SCI - Hasta el 8 de marzo

# Múltiples vulnerabilidades en UPS CS141 de Generex

---

INCIBE ha coordinado la publicación de 7 vulnerabilidades en el adaptador UPS CS141 de Generex, que han sido descubiertas por Joel Gámez Molina (@JoelGMSec).

Avisos SCI - Hasta el 8 de marzo

# [Actualización 03/03/2023] Múltiples vulnerabilidades en UPS CS141 de Generex

---

INCIBE ha coordinado la publicación de 7 vulnerabilidades en el adaptador UPS CS141 de Generex, que han sido descubiertas por Joel Gámez Molina (@JoelGMSec).

Avisos SCI - Hasta el 8 de marzo

# Múltiples vulnerabilidades en PTC ThingWorx Edge

---

Los investigadores, Chris Anastasio y Steven Seeley, de Incite Team, han reportado 2 vulnerabilidades críticas en ThingWorx Edge de PCT, cuya explotación podría permitir a un atacante bloquear el dispositivo afectado o provocar una condición de denegación de servicio (DoS).

Avisos SCI - Hasta el 8 de marzo

# Múltiples vulnerabilidades en la implementación de DDS

---

Amrc-benmorrow, Gianluca Caizza, Ruffin White, Victor Mayoral Vilches y Mikael Arguedas han reportado a Alias Robotics 3 vulnerabilidades de severidad alta, que podrían permitir a un atacante comprometer y obtener el control total de los sistemas afectados.

Avisos SCI - Hasta el 8 de marzo

# Múltiples vulnerabilidades en NetMan 204 de Riello UPS

---

INCIBE ha coordinado la publicación de 3 vulnerabilidades en NetMan 204 de Riello UPS, que han sido descubiertas por Joel Gámez Molina (@JoelGMSec).

Avisos SCI - Hasta el 8 de marzo



# Múltiples vulnerabilidades en productos de WAGO

---

Ryan Pickren, investigador de Georgia Institute of Technology's Cyber-Physical Security Lab, coordinado por el CERT@VDE, ha detectado cuatro vulnerabilidades: dos de severidad crítica y dos de severidad media basadas en la gestión web (WBM) del controlador lógico programable de (PLC).

Avisos SCI - Hasta el 8 de marzo

# Vulnerabilidades en productos Gateway Station de Hitachi Energy

---

Se han detectado 5 vulnerabilidades de severidad alta. La explotación exitosa de estas vulnerabilidades podría provocar que los módulos afectados dejen de funcionar o que parte de GWS no se inicie, permitir ejecución de código, sin autenticación, o denegación de servicio (DoS).

Avisos SCI - Hasta el 8 de marzo

# Autenticación incorrecta en ABB Ability Symphony Plus

---

ABB ha identificado una vulnerabilidad, de severidad alta, que podría permitir a un cliente no autorizado conectarse a los servidores de S+ Operations para actuar como un cliente legítimo.

Avisos SCI - Hasta el 8 de marzo

# Divulgación de información en MELSEC iQ-F Series de Mitsubishi Electric

---

JeongHoon Bae, YiJoon Jung, JinYoung Kim, HyeokJong Yun y HeeA Go, de HelloT, han reportado una vulnerabilidad de severidad alta, que podría permitir a un atacante no autenticado obtener credenciales en texto plano.

Avisos SCI - Hasta el 8 de marzo

# Inyección de comandos en productos de Baicells

---

Rustam Amin ha informado de una vulnerabilidad de severidad crítica que podría permitir que los comandos se ejecuten antes del inicio de sesión y con permisos de root.

Avisos SCI - Hasta el 8 de marzo

# Vulnerabilidad DoS en dispositivos de Phoenix Contact usados por Bosch

---

Los dispositivos FL MGUARD y TC MGUARD, del fabricante Phoenix Contact, están a la venta por parte de Bosch Rexroth como productos comerciales. En dichos dispositivos, se ha identificado una vulnerabilidad de severidad alta cuya explotación podría causar una condición de denegación de servicio (DoS).

Avisos SCI - Hasta el 8 de marzo

# Múltiples vulnerabilidades en productos de Phoenix Contact

---

ONEKEY ha reportado dos vulnerabilidades de severidad alta en los dispositivos afectados, cuya explotación podría permitir a un atacante ejecutar comandos arbitrarios, cargar archivos arbitrarios o eliminar archivos del dispositivo, pudiendo provocar que el funcionamiento no sea el adecuado.

Avisos SCI - Hasta el 8 de marzo

# Múltiples vulnerabilidades en Serie MXsecurity de Moxa

---

SSimon Janz ha reportado dos vulnerabilidades a Moxa: una de severidad crítica, que podría permitir la ejecución de comandos y otra de severidad alta, que podría eludir credenciales codificadas.

Avisos SCI - Hasta el 8 de marzo