

Del 8 al 22 de septiembre

# AVISOS SCI



# Múltiples vulnerabilidades en Socomec MOD3GP-SY-120K

---

El investigador, Aarón Flecha Menéndez, ha reportado 7 vulnerabilidades detectadas en el producto MOD3GP-SY-120K de Socomec, 1 de severidad crítica, 4 altas y 2 medias. La explotación de estas vulnerabilidades podría permitir a un atacante ejecutar código JavaScript malicioso, obtener información sensible o robar cookies de sesión.

Avisos SCI - Del 8 al 22 de septiembre

# Múltiples vulnerabilidades en MAGLINK LX Web Console de Dover Fueling Solutions

---

Soufian El Yadmani, de Darktrace/CSIRT.global, ha reportado 3 vulnerabilidades: una de severidad crítica, otra de severidad alta y otra de severidad media, que podrían permitir a un atacante obtener acceso completo al sistema afectado.

Avisos SCI - Del 8 al 22 de septiembre

# Vulnerabilidad de falta de autenticación en el servicio de actualización del IGSS de Schneider Electric

---

Sina Kheirkhah (@SinSinology), de Summoning Team, en colaboración con Trend Micro Zero Day Initiative, ha reportado una vulnerabilidad de severidad alta, cuya explotación podría permitir a un atacante remoto llevar a cabo una ejecución remota de código.



# Avisos de seguridad de Siemens de septiembre de 2023

---

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

Avisos SCI - Del 8 al 22 de septiembre

# [Actualización 22/09/2023] Avisos de seguridad de Siemens de septiembre de 2023

---

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

Avisos SCI - Del 8 al 22 de septiembre

# Múltiples vulnerabilidades en WIBU Codemeter de Trumpf

---

CERT@VDE en coordinación con TRUMPF, ha publicado 2 vulnerabilidades: una de severidad alta, y otra crítica, que podrían generar una elevación de privilegios y acceso completo en la estación de trabajo para un usuario ya autenticado.

Avisos SCI - Del 8 al 22 de septiembre

# Autenticación incorrecta en Pavilion8 de Rockwell Automation

---

Rockwell Automation ha informado de una vulnerabilidad de severidad alta que podría permitir a un atacante recuperar datos de sesiones de otros usuarios.

Avisos SCI - Del 8 al 22 de septiembre



# Vulnerabilidades en WIBU-SYSTEMS impactan en productos Phoenix Contact

---

Phoenix Contact, con la coordinación y el soporte del CERT@VDE, ha informado de 2 vulnerabilidades: una de severidad crítica y otra alta, que afectan a varios productos. Estas vulnerabilidades, de tipo denegación de servicio (DoS), se encuentran en CodeMeter de WIBU-SYSTEMS, que está incorporado en los productos afectados de Phoenix Contact.

Avisos SCI - Del 8 al 22 de septiembre

# Vulnerabilidad de ejecución de código en GX Works3 de Mitsubishi Electric

---

01dGu0, de Zhejiang Qian Information & Technology Co., Ltd., ha reportado una vulnerabilidad de severidad crítica, cuya explotación podría permitir a un atacante local ejecutar código malicioso.

# Control inadecuado de la frecuencia de interacción en productos de Omron

---

Reid Wightman, de Dragos, ha reportado una vulnerabilidad de severidad alta, cuya explotación podría permitir a un atacante obtener información sensible en memoria.

# Múltiples vulnerabilidades en productos de Ingeteam

---

INCIBE ha coordinado la publicación de 3 vulnerabilidades que afectan a INGEPAC DA 3451 e INGEPAC EF MD de Ingeteam, descubiertas por los investigadores de ciberseguridad industrial Aarón Flecha Menéndez y Gabriel Vía Echezarreta.

A estas vulnerabilidades se les han asignado los siguientes códigos, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE de cada vulnerabilidad.

Avisos SCI - Del 8 al 22 de septiembre



# Múltiples vulnerabilidades en Frauscher FDS101

---

Frauscher Sensortechnik, en coordinación con el CERT@VDE, ha informado de 3 vulnerabilidades, de severidades crítica, alta y media, cuya explotación podría conllevar un compromiso total del dispositivo FDS101 afectado.

Avisos SCI - Del 8 al 22 de septiembre

# Cross-Site Scripting en la serie 460 de Real Time Automation

---

CISA ha reportado una vulnerabilidad de severidad crítica, tras descubrir una prueba de concepto pública de la que es autor Yehia Elghaly, cuya explotación podría permitir a un atacante ejecutar contenido JavaScript malicioso, resultando en un Cross-Site Scripting (XSS).

Avisos SCI - Del 8 al 22 de septiembre

# Escritura fuera de límites en DIAScreen de Delta Electronics

---

Kimiya, en colaboración con Trend Micro Zero Day Initiative, ha reportado una vulnerabilidad de severidad alta, cuya explotación podría permitir la ejecución remota de código.

Avisos SCI - Del 8 al 22 de septiembre