

Hasta el 3 de abril

AVISOS SCI



Asignación de permisos incorrectos en RoboDK

Noam Moshe de Claroty ha informado de una vulnerabilidad de severidad alta, cuya explotación podría permitir que un atacante aumente los privilegios y así, escribir archivos en el directorio de RoboDK y lograr la ejecución del código.

Avisos SCI - Hasta el 3 de abril

Múltiples vulnerabilidades en controladores de bomba Osprey de ProPump

Gjoko Krstic, de Zero Science Lab, ha informado de 9 vulnerabilidades: 4 de ellas de severidad crítica y 5 de severidad alta. Su explotación podría permitir que un atacante obtenga acceso no autorizado, recupere información confidencial, modifique datos, provoque una denegación de servicio y/o obtenga control administrativo.

Avisos SCI - Hasta el 3 de abril

Múltiples vulnerabilidades en productos de estaciones de automatización de edificios de SAUTER

Ithaca Labs, de Odyssey Cyber Security, ha informado de 5 vulnerabilidades: 4 de severidad alta y 1 de severidad media. La explotación de estas vulnerabilidades podría dar lugar a una escalada de privilegios, la ejecución no autorizada de acciones, una condición de denegación de servicio o la recuperación de información confidencial.

Avisos SCI - Hasta el 3 de abril

Protección de credenciales insuficiente en KVMS Pro de CP Plus

Harshit Shukla ha informado de una vulnerabilidad de severidad alta que podría permitir a un atacante recuperar credenciales confidenciales y controlar todo el sistema de CCTV.

Avisos SCI - Hasta el 3 de abril

Credenciales por defecto en ABB RCCMD

Pablo Valle Alvear, investigador de Titanium Industrial Security, ha reportado una vulnerabilidad crítica en productos RCCMD (Remote Control Command) de ABB. Un atacante podría provocar el acceso legítimo a un nodo del sistema afectado, la detención del mismo de forma remota, tomar el control e insertar y ejecutar código arbitrario en el nodo.

Avisos SCI - Hasta el 3 de abril

Inyección de comandos en Altenergy Power System Control Software de APsystems

Se ha detectado una vulnerabilidad de severidad crítica en Altenergy Power System Control Software, software de control de microinversores de APsystems, cuya explotación podría permitir a un atacante realizar una escalada de privilegios. Adicionalmente, se tiene constancia de la divulgación de una PoC (Proof of Concept) que permitiría la explotación de esta vulnerabilidad.

Avisos SCI - Hasta el 3 de abril

Múltiples vulnerabilidades en productos AC500 de ABB

Se han identificado 21 vulnerabilidades en varias versiones del producto AC500 del fabricante ABB, una de ellas de severidad crítica y el resto repartidas entre altas y medias. La explotación de estas vulnerabilidades podría permitir a un atacante una interrupción o inaccesibilidad del sistema afectado, una condición de denegación de servicio o una sobrescritura de memoria local.

Avisos SCI - Hasta el 3 de abril

Vulnerabilidad SQLi en Contec CHS

Tenable, en coordinación con JPCERT y el fabricante Contec, ha informado de una vulnerabilidad de severidad alta que afecta a CONPROSYS HMI System (CHS) y cuya explotación podría permitir a un atacante obtener información de la base de datos de CHS.

Avisos SCI - Hasta el 3 de abril

Múltiples vulnerabilidades en productos de Autodesk

Mat Powell de Trend Micro Zero Day Initiative, y cbgabriel junto al MSRC team, han informado de 6 vulnerabilidades de severidad alta. La explotación de estas vulnerabilidades podría permitir a un atacante realizar una ejecución de código, una denegación de servicio o una divulgación de información.

Avisos SCI - Hasta el 3 de abril