
# Boletín de junio de 2020

## Avisos de Sistemas de Control Industrial

## Desbordamiento de búfer en Point-to-Point Protocol Daemon

**Fecha de publicación:** 02/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Demonio pppd (*Point to Point Protocol Daemon*), desde la versión 2.4.2, hasta la 2.4.8.

- Fabricantes afectados:
  - Phoenix Conctac:
    - dispositivos FL MGUARD, TC MGUARD, TC ROUTER y TC CLOUD CLIENT.

**Descripción:**

El investigador Ilja Van Sprundel, de IOActive, ha detectado una vulnerabilidad de severidad crítica que afecta al demonio pppd. Un atacante remoto, no autenticado, podría realizar un desbordamiento de búfer y, de este modo, ejecutar código arbitrario en el sistema.

**Solución:**

Aplicar el último parche disponible de pppd en función de las configuraciones que se dispongan en este. Para obtener más información, consultar el apartado Referencias.

**Detalle:**

Debido a un fallo en el procesado de paquetes de *Extensible Authentication Protocol* (EAP) en el demonio pppd, un atacante remoto, no autenticado, podría realizar un desbordamiento de búfer que podría permitirle ejecutar código arbitrario en el sistema. Se ha asignado el identificador CVE-2020-8597 para esta vulnerabilidad.

**Etiquetas:** Actualización, Comunicaciones, Vulnerabilidad

## Falta de autenticación en función crítica en Grid Solutions Reason RT Clocks de GE

**Fecha de publicación:** 03/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Grid Solutions Reason RT Clocks RT430, RT431 y RT434, todas las versiones de *firmware* anteriores a 08A05.

**Descripción:**

Ehab Hussein, de IOActive, reportó al fabricante GE una vulnerabilidad, de severidad crítica, de falta de autenticación en función crítica, en varias versiones de Grid Solutions Reason RT Clocks.

**Solución:**

El fabricante recomienda actualizar la versión de *firmware* de los productos afectados a 08A05.

**Detalle:**

La vulnerabilidad podría permitir que un atacante, no autenticado, ejecute comandos arbitrarios y envíe una solicitud a una URL específica

que podría hacer que el dispositivo deje de responder. Podría cambiar la contraseña de la cuenta de usuario de *configuration*, permitiendo de esta manera la modificación de la configuración del dispositivo a través de la interfaz web utilizando la nueva contraseña, o también podría omitir la autenticación requerida para configurar el dispositivo y reiniciar el sistema. Se ha asignado el identificador CVE-2020-12017 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Gestión inadecuada de contraseñas en productos PACTware

**Fecha de publicación:** 03/06/2020

**Importancia:** Alta

**Recursos afectados:**

PACTware, versiones:

- 5.0.4.xx y anteriores;
- 4.1 SP5 y anteriores;
- 3.X y anteriores;
- 2.4 y anteriores.

**Descripción:**

Reid Wightman, de Dragos Inc, coordinado por [email protected] y BSI, ha reportado dos vulnerabilidades en la gestión de contraseñas de los productos afectados.

**Solución:**

Actualizar a las versiones PACTware 5.0.5.31, PACTware 4.1 SP6 o superiores.

**Detalle:**

PACTware permite "roles de usuario", que limitan el acceso de acuerdo con las directrices de la FDT. Sin embargo, por defecto no se establecen contraseñas y el usuario tiene el rol de 'admin' sin ningún tipo de limitación.

Si el usuario habilita el control de acceso a los roles, cada rol puede ser protegido con una contraseña individual.

- Estos ajustes pueden ser modificados por un usuario local sin ninguna verificación, lo que podría permitir modificar la habilitación del rol, y las contraseñas de los roles, sin necesidad de autenticarse previamente. Se ha reservado el identificador CVE-2020-9404 para esta vulnerabilidad.
- Los ajustes pueden ser leídos por un usuario local sin verificación. Es posible recuperar las contraseñas de los roles, si las contraseñas fueron establecidas previamente. Se ha reservado el identificador CVE-2020-9403 para esta vulnerabilidad.

Si el usuario no ha habilitado los roles individuales, un atacante puede habilitar los roles y asignarles contraseñas. Esto podría impedir que los usuarios legítimos utilizaran el *software*.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Inyección de comandos en VPort461 de Moxa

**Fecha de publicación:** 08/06/2020

**Importancia:** Alta

**Recursos afectados:**

Dispositivos Vport 461, con versión de firmware 3.4 o inferior.

**Descripción:**

El investigador Xinjie Ma, de Beijin Chaitin Future Technology Co.,Ltd. , reportó una vulnerabilidad del tipo inyección de comandos que afecta a los dispositivos VPort 461 Series Industrial Video Servers.

**Solución:**

Moxa ha solicitado a los clientes afectados que se pongan en contacto con su servicio de soporte técnico para recibir la actualización que soluciona el problema.

**Detalle:**

Una vulnerabilidad en el dispositivo podría permitir a un atacante remoto la ejecución de comandos arbitrarios.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Vulnerabilidad de consumo de recursos no controlado en dispositivos MELSEC iQ-R de Mitsubishi Electric

**Fecha de publicación:** 10/06/2020

**Importancia:** Media

**Recursos afectados:**

Dispositivos MELSEC iQ-R:

- R04/08/16/32/120CPU, R04/08/16/32/120ENCPU, con versiones de firmware 39 y anteriores;
- R00/01/02CPU, con versiones de firmware 7 y anteriores;
- R08/16/32/120SFCPU, con versiones de firmware 20 y anteriores;
- R08/16/32/120PCPU, todas las versiones;
- R08/16/32/120PSFCPU, todas las versiones;
- RJ71EN71, todas las versiones.

**Descripción:**

El investigador Yossi Reuven, de SCADAfecnce, ha reportado a Mitsubishi Electric una vulnerabilidad de severidad media, del tipo consumo de recursos no controlado.

**Solución:**

Mitsubishi Electric recomienda emplear un firewall para bloquear el acceso a los dispositivos afectados desde redes y dispositivos no confiables.

También es recomendable el uso de redes virtuales privadas (VPNs) como método de acceso remoto a los dispositivos.

**Detalle:**

La vulnerabilidad podría generar en el puerto Ethernet del dispositivo una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2020-13238 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Vulnerabilidad de desbordamiento de búfer en Advantech WebAccess Node

**Fecha de publicación:** 10/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Advantech WebAccess Node, versión 8.4.4 y anteriores.

**Descripción:**

Z0mb1E, trabajando con Zero Day Initiative de Trend Micro, reportó una vulnerabilidad al CISA, de severidad crítica, de tipo desbordamiento de búfer basado en pila (*stack*).

**Solución:**

El fabricante ha publicado el parche P0520844 para solucionar esta vulnerabilidad.

**Detalle:**

El producto afectado es vulnerable a un desbordamiento de búfer basado en pila (*stack*), lo que podría permitir a un atacante remoto ejecutar código arbitrario. Se ha reservado el identificador CVE-2020-12019 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Boletín de seguridad de Siemens de junio de 2020

**Fecha de publicación:** 10/06/2020

**Importancia:** Crítica

**Recursos afectados:**

- LOGO!8 BM (incluidas las variantes SIPLUS), todas las versiones;
- SIMATIC Automation Tool, todas las versiones;
- SIMATIC NET PC software, todas las versiones desde la v16, anteriores a la v16 Upd3;
- SIMATIC PCS 7, todas las versiones;
- SIMATIC PCS neo, todas las versiones;
- SIMATIC ProSave, todas las versiones;
- SIMATIC S7-1500 Software Controller, todas las versiones;
- SIMATIC STEP 7, todas las versiones anteriores a la v5.6 SP2 HF3;
- SIMATIC STEP 7 (TIA Portal) v13, todas las versiones;
- SIMATIC STEP 7 (TIA Portal) v14, todas las versiones;
- SIMATIC STEP 7 (TIA Portal) v15, todas las versiones;
- SIMATIC STEP 7 (TIA Portal) v16, todas las versiones;
- SIMATIC WinCC OA v3.16, todas las versiones anteriores a la P018;
- SIMATIC WinCC OA v3.17, todas las versiones anteriores a la P003;
- SIMATIC WinCC Runtime Professional v13, todas las versiones;
- SIMATIC WinCC Runtime Professional v14, todas las versiones;
- SIMATIC WinCC Runtime Professional v15, todas las versiones;
- SIMATIC WinCC Runtime Professional v16, todas las versiones;

- SIMATIC WinCC v7.4, todas las versiones anteriores a la v7.4 SP1 Update 14;
- SIMATIC WinCC v7.5, todas las versiones anteriores a la v7.5 SP1 Update 3;
- SINAMICS Startdrive, todas las versiones;
- SINEC NMS, todas las versiones;
- SINEMA Server, todas las versiones;
- SINUMERIK ONE virtual, todas las versiones;
- SINUMERIK Operate, todas las versiones;
- SIMATIC PDM, todas las versiones;
- SIMATIC STEP 7 v5.X, todas las versiones anteriores a la 5.6 SP2 HF3;
- SINAMICS STARTER (incluido STEP 7 OEM), todas las versiones anteriores a la 5.4 HF1;
- SINUMERIK Access MyMachine/P2P, todas las versiones anteriores a la 4.8;
- SINUMERIK PCU base Win10 software/IPC, todas las versiones anteriores a la 14.00;
- SINUMERIK PCU base Win7 software/IPC, todas las versiones anteriores a la 12.01 HF4;

**Descripción:**

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

**Solución:**

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden obtenerse desde el panel de descarga de Siemens. Para los productos sin actualizaciones disponibles hay que aplicar las medidas de mitigación descritas en la sección de Referencias.

**Detalle:**

Siemens, en su comunicación mensual de parches de seguridad, ha emitido un total de 7 avisos de seguridad, de las cuales 3 son actualizaciones.

Los tipos de nuevas vulnerabilidades publicadas se corresponden con los siguientes:

- 1 vulnerabilidad de ausencia de autenticación en función crítica,
- 1 vulnerabilidad de elemento o ruta de búsqueda sin entrecomillar,
- 1 vulnerabilidad de elemento no controlado en la ruta de búsqueda,
- 6 vulnerabilidades de desbordamiento de búfer basado en memoria dinámica (Heap),
- 4 vulnerabilidades de desbordamiendo de búfer basado en pila (Stack),
- 4 vulnerabilidades de lectura fuera de límites,
- 2 vulnerabilidades de inicialización inapropiada,
- 3 vulnerabilidades de acceso a una ubicación de memoria después del final del búfer,
- 1 vulnerabilidad de referencia a una ubicación de memoria antes del comienzo del búfer,
- 2 vulnerabilidades de error en el cálculo de longitud por exceso o defecto de una unidad (off-by-one),
- 1 vulnerabilidad de terminación null incorrecta.

Para estas vulnerabilidades se han reservado los siguientes identificadores: CVE-2020-7589, CVE-2020-7580, CVE-2020-7585, CVE-2020-7586, CVE-2018-15361, CVE-2019-8258, CVE-2019-8259, CVE-2019-8260, CVE-2019-8261, CVE-2019-8262, CVE-2019-8263, CVE-2019-8264, CVE-2019-8265, CVE-2019-8266, CVE-2019-8267, CVE-2019-8268, CVE-2019-8269, CVE-2019-8270, CVE-2019-8271, CVE-2019-8272, CVE-2019-8273, CVE-2019-8274, CVE-2019-8275, CVE-2019-8276, CVE-2019-8277 y CVE-2019-8280.

**Etiquetas:** Actualización, Siemens, Vulnerabilidad

---

# Boletín de seguridad de Schneider Electric de junio de 2020

**Fecha de publicación:** 10/06/2020

**Importancia:** Crítica

**Recursos afectados:**

- Modicon M218, versión de *firmware* 4.3 y anteriores;
- Unity Loader, todas las versiones;
- OS Loader, todas las versiones;
- Modicon LMC078 Logic Controller, versión de *firmware* 1.51.15.05 y posteriores.

**Descripción:**

El CNCERT y el investigador Yang Dong, perteneciente a DingXiang Dongjian Security Lab, han reportado a Schneider Electric 3 vulnerabilidades, de severidades crítica, alta y media, y de tipo uso de credenciales en claro, desreferencia a puntero nulo y escritura fuera de límites, respectivamente.

**Solución:**

Seguir las instrucciones de actualización y configuración descritas en la sección *Remediation / Available Remediations* de cada aviso del fabricante.

**Detalle:**

Un atacante que aproveche estas vulnerabilidades podría realizar las siguientes acciones:

- acceso no autorizado al servicio de transferencia de archivos provisto por los PLC Modicon;
- el componente IGMP en los parches IPNET CVE de VxWorks 6.8.3 creados en 2019 tiene una referencia de puntero nulo;
- denegación de servicio cuando se envían paquetes específicos TCP/IP, especialmente diseñados, al controlador lógico Modicon M218.

Para estas vulnerabilidades, se han reservado los identificadores: CVE-2020-7498 y CVE-2020-7502, y se ha asignado CVE-2020-10664.

**Etiquetas:** Actualización, Infraestructuras críticas, Schneider Electric, Vulnerabilidad

---

# Gestión de privilegios inadecuada en múltiples productos de WAGO

**Fecha de publicación:** 11/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Todas las versiones de *firmware* de los siguientes productos:

- Series PFC100 (750-81xx/xxx-xxx),
- Series PFC200 (750-82xx/xxx-xxx),
- 762-4xxx Wago Touch Panel 600 Standard Line,
- 762-5xxx Wago Touch Panel 600 Advanced Line,
- 762-6xxx Wago Touch Panel 600 Marine Line.

**Descripción:**

El investigador, Kelly Leuschner de la empresa Cisco Talos, coordinado por el [email protected], ha identificado una vulnerabilidad, de severidad crítica, de tipo gestión inadecuada de privilegios en distintos productos de WAGO, que ha reportado al propio fabricante.

**Solución:**

En versiones anteriores de los manuales de productos de WAGO, se hizo una distinción entre WBM y el sistema Linux. Esta información era incorrecta y WAGO la ha corregido en las versiones actuales de los manuales, que se actualizarán en junio de 2020. Válido desde la versión de *firmware* 03.04.10 (16) / capítulo 5.1.2.1.2.

**Detalle:**

Un atacante autenticado que tenga acceso a WBM (*Web Based Management*) podría usar la funcionalidad de carga de *software* para instalar un paquete de *software* con privilegios de *root*. Este hecho podría permitirle manipular el dispositivo u obtener el control del mismo. Se ha reservado el identificador CVE-2020-6090 para esta vulnerabilidad.

**Etiquetas:** Infraestructuras críticas, Vulnerabilidad

---

# Múltiples vulnerabilidades en varios productos de Rockwell Automation

**Fecha de publicación:** 12/06/2020

**Importancia:** Crítica

**Recursos afectados:**

- FactoryTalk Linx, versiones 6.00, 6.10 y 6.11;
- RSLinx Classic, versión 4.11.00 y anteriores;
- lSharon Brizinov and Amir Preminger (VP Research) of Clarotyos siguientes productos, que utilizan FactoryTalk Linx Software:
  - Connected Components Workbench, versión 12 y anteriores;
  - ControlFLASH, versión 14 y posteriores;
  - ControlFLASH Plus, versión 1 y posteriores;
  - FactoryTalk Asset Centre, versión 9 y posteriores;
  - FactoryTalk Linx CommDTM, versión 1 y posteriores;
  - Studio 5000 Launcher, versión 31 y posteriores;
  - Studio 5000 Logix Designer software, versión 32 y posteriores.

**Descripción:**

Sharon Brizinov y Amir Preminger, de Claroty, han reportado 4 vulnerabilidades al CISA y a Rockwell Automation, 2 con severidad crítica y 2 altas, de tipo validación incorrecta de datos de entrada, acceso a rutas no controlado y carga sin restricción de ficheros peligrosos.

**Solución:**

El fabricante recomienda aplicar los siguientes parches:

- Patch Roll-up para CPR9 SRx,
- FactoryTalk Linx/Services patch RAID# 1124820,
- FactoryTalk Linx patch RAID# 1126433.

**Detalle:**

- Una llamada expuesta a la API permite a los usuarios proporcionar archivos para procesar sin sanitizar. Esto podría permitir que un atacante especifique un nombre de archivo para ejecutar código no autorizado y modificar archivos o datos. Se ha reservado el identificador CVE-2020-11999 para esta vulnerabilidad.
- El mecanismo de análisis que procesa ciertos tipos de archivos no proporciona proceso de sanitización de entrada. Esto podría permitir que un atacante use archivos especialmente diseñados para recorrer el sistema de archivos, modificar o exponer datos confidenciales, o ejecutar código arbitrario. Se ha reservado el identificador CVE-2020-12001 para esta vulnerabilidad.
- Una llamada expuesta a la API permite a los usuarios proporcionar archivos para procesar sin sanitizar. Esto podría permitir que un atacante use solicitudes, especialmente diseñadas, para recorrer el sistema de archivos y exponer datos confidenciales en el disco duro local. Se ha reservado el identificador CVE-2020-12003 para esta vulnerabilidad.
- Existe una vulnerabilidad en la función de comunicación que permite a los usuarios cargar archivos EDS por FactoryTalk Linx. Esto podría permitir que un atacante cargue un archivo con mala compresión, consumiendo todos los recursos de CPU disponibles, lo que generaría una condición de denegación de servicio. Se ha reservado el identificador CVE-2020-12005 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Vulnerabilidad en IntelliBridge Enterprise (IBE) de Philips

**Fecha de publicación:** 12/06/2020

**Importancia:** Baja

**Recursos afectados:**

- IntelliBridge Enterprise (IBE) versiones B.12 y anteriores.
- Tambien se ve afectada la integración del sistema de IntelliBridge Enterprise con:
  - SureSigns (VS4),
  - EarlyVue (VS30),
  - IntelliVue Guardian (IGS).

**Descripción:**

Se ha publicado una vulnerabilidad que podría permitir a un atacante leer credenciales de texto plano de los archivos de registro.

**Solución:**

- El fabricante tiene prevista una nueva versión (IBE B.13) para el Q4 de 2020 que solucione esta vulnerabilidad.
- Como una mitigación provisional de esta vulnerabilidad, Philips recomienda:
  - Los registros de transacciones de la IBE sólo son accesibles con privilegios administrativos. Se puede crear una cuenta adicional en el sistema IBE con privilegios limitados, para los ingenieros de servicio.
  - Reducir la retención de los registros a un plazo aceptable que permita las actividades de recuperación.

**Detalle:**

Las credenciales de usuario no codificadas recibidas en IntelliBridge Enterprise (IBE) se registran en los registros de transacciones, que están seguros detrás del portal web administrativo de acceso. Las credenciales de usuario no cifradas enviadas desde los productos afectados, a efectos del *handsake* o de autenticación con el Enterprise Systems, se registran como la carga útil en IntelliBridge Enterprise (IBE) dentro de los registros de transacciones. Un atacante con privilegios administrativos podría explotar esta vulnerabilidad para leer credenciales de texto plano de los archivos de registro. Se ha asignado el identificador CVE-2020-12023 para esta vulnerabilidad.

**Etiquetas:** Infraestructuras críticas, Vulnerabilidad

---

# Vulnerabilidad de Cross-site Scripting en PI Web API de OSIsoft

**Fecha de publicación:** 12/06/2020

**Importancia:** Alta

**Recursos afectados:**

PI Web API 2019 Patch 1 (1.12.0.6346) y todas las versiones anteriores.

**Descripción:**

OSIsoft junto con Dor Yardeni y Eliad Mualem, de OTORIO, han reportado una vulnerabilidad de Cross-site Scripting que podría permitir a un atacante la ejecución remota de código arbitrario.

**Solución:**

Actualizar a la versión PI Web API 2019 SP1.

**Detalle:**

Una vulnerabilidad de Cross-site Scripting en PI Web API de OSIsoft podría permitir a un atacante la ejecución remota de código arbitrario. Se ha asignado el identificador CVE-2020-12021 para esta vulnerabilidad.

**Etiquetas:** Actualización, Vulnerabilidad

---

# Desbordamiento de búfer en múltiples productos de Moxa

**Fecha de publicación:** 15/06/2020

**Importancia:** Alta

**Recursos afectados:**

Routers EDR-G902 Series y EDR-G903 Series, versiones 5.4 y anteriores.

**Descripción:**

Tal Keren, de Claroty, ha reportado una vulnerabilidad, de tipo desbordamiento de búfer basado en pila (*stack*), que afecta a varios routers de Moxa.

**Solución:**

Actualizar el *firmware* a la versión 5.5 de EDR-G902 Series y EDR-G903 Series.

**Detalle:**

El funcionamiento malicioso de la cookie del navegador web, podría permitir a un atacante el desbordamiento del búfer de pila (*stack*) en el servidor web del sistema mediante el uso de una cookie especialmente diseñada.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Múltiples vulnerabilidades en la implementación de protocolos Treck IP

**Fecha de publicación:** 17/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Los productos afectados son aquellos que implementan versiones anteriores a Treck TCP/IP 6.0.1.66

En concreto afectando a los siguientes protocolos:

- IPv4,
- IPv6,
- UDP,
- DNS,
- DHCP,
- TCP,
- ICMPv4,
- ARP,

Algunos fabricantes afectados son:

- B.Braun,
- Caterpillar,
- Green Hills,
- Rockwell,
- Schneider Electric,

Puede consultar la lista completa de fabricantes afectados en la sección *Referencias*, o en el siguiente en enlace.

**Descripción:**

Los investigadores, Shlomi Oberman y Moshe Kol, de JSOF Tech, han reportado varias vulnerabilidades conocidas como 'Ripple20' en la implementación de protocolos Treck IP desarrollada por Treck Inc., e incluida en productos de diversos fabricantes.

**Solución:**

Treck recomienda a los usuarios aplicar la versión 6.0.1.66 o superior de su implementación Treck TCP/IP. Se puede obtener más información en su página web.

**Detalle:**

Se han descubierto un total de 19 vulnerabilidades que afectan a la implementación de protocolos Treck IP. Siendo 4 de ellas críticas y pudiendo suponer una ejecución remota de código o escritura fuera de los límites de memoria en diferentes implementaciones.

Los identificadores CVE de las vulnerabilidades son: CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913 y CVE-2020-11914.

**Etiquetas:** Actualización, Infraestructuras críticas, IoT, SCADA, Schneider Electric, Vulnerabilidad

---

# Vulnerabilidad en controladores de red TwinCAT RT de Beckhoff

**Fecha de publicación:** 17/06/2020

**Importancia:** Media

**Recursos afectados:**

- Controlador TwinCAT para Intel 8254x:
  - Versión < = 3.1.0.3603 para TwinCAT 3.1 4024;
  - Versión < = 3.1.0.3512 para TwinCAT 3.1 4022;
  - Versión < = 2.11.0.2120 para TwinCAT 2.11 2350.
- Controlador TwinCAT para Intel 8255x:
  - Versión < = 3.1.0.3600 para TwinCAT 3.1 402;
  - Versión < = 3.1.0.3500 para TwinCAT 3.1 4024;
  - Versión < = 2.11.0.2117 para TwinCAT 2.11 2350.
- Estos están incluidos en las versiones de TwinCAT anteriores o iguales a:
  - TwinCAT 3.1 4024.10;
  - TwinCAT 3.1 4022.32;
  - TwinCAT 2.11 2305.
- A su vez, estas versiones se incluyen en las siguientes imágenes:
  - Todos los PCs integrados (CX) con Windows 7 / 10 / CE;

- Todos los PCs industriales con Windows 7 / 10 / CE, en caso de que el controlador TwinCAT RT estuviera activado.

**Descripción:**

Beckhoff ha reportado al [email protected] una vulnerabilidad del tipo revelación de información en el controlador de red TwinCAT RT de Beckhoff para Intel 8254x y 8255x.

**Solución:**

- Si no se requiere una comunicación en tiempo real desde el TwinCAT en la interfaz Ethernet, los usuarios pueden reconfigurarlos, de forma alternativa, para usar el controlador Intel, que se envía con las imágenes de Beckhoff.
- Los clientes deben configurar un cortafuegos perimetral para bloquear el tráfico de las redes no confiables al dispositivo, especialmente en lo que respecta a ICMP y otros frames ethernet.
- Beckhoff ofrece parches de software para TwinCAT 3.1 y TwinCAT 2.11 bajo demanda. Estos parches se incluirán en las próximas versiones del software afectado.

**Detalle:**

El controlador de red TwinCAT RT de Beckhoff para Intel 8254x y 8255x cuenta con la funcionalidad EtherCAT e implementa características en tiempo real. Excepto las tramas de Ethernet enviadas desde la funcionalidad en tiempo real, todas las demás tramas de Ethernet enviadas a través del controlador no presentan *padding* si su payload es menor que el tamaño mínimo de trama Ethernet. En cambio, el contenido de la memoria arbitraria se transmite dentro de los bytes de *padding*. Lo más probable es que esta memoria contenga fragmentos de frames previamente transmitidos o recibidos. Se ha asignado el identificador CVE-2020-12494 para esta vulnerabilidad.

**Etiquetas:** Vulnerabilidad

---

# Múltiples vulnerabilidades en robots KUKA

**Fecha de publicación:** 18/06/2020

**Importancia:** Alta

**Recursos afectados:**

Robots KUKA bajo sistemas KR3R540, KRC4, KSS8.5.7HF1 y Win7_Embedded.

**Descripción:**

El investigador Víctor Mayoral Vilches, de Alias Robotics, ha descubierto varias vulnerabilidades de severidad alta en sistemas utilizados por robots KUKA.

**Solución:**

Actualmente no hay actualizaciones que solucionen las vulnerabilidades.

Se recomienda limitar el acceso físico a los dispositivos para evitar que se puedan manipular.

**Detalle:**

Las vulnerabilidades encontradas podrían permitir a un atacante, con acceso físico al sistema, alterar servicios críticos para la operación desde el administrador de tareas de Windows, deteniendo el manipulador.

Además, los sistemas afectados cuentan con chips DRAM afectados por la vulnerabilidad conocida como *TRRespass*, que supone que en los mismos todavía se pueden efectuar ataques de tipo *RowHammer*.

Los identificadores asignados de estas vulnerabilidades son CVE-2020-10255 y CVE-2020-10268.

**Etiquetas:** Vulnerabilidad

---

# Vulnerabilidad en exacqVision de Johnson Controls

**Fecha de publicación:** 19/06/2020

**Importancia:** Alta

**Recursos afectados:**

- exacqVision Web Service, versión 20.03.2.0 y anteriores;
- exacqVision Enterprise Manager, versión 20.03.3.0 y anteriores.

**Descripción:**

Una vulnerabilidad en exacqVision, de tipo verificación incorrecta de la firma criptográfica, podría permitir a un atacante, con privilegios de administrador, la ejecución de comandos del sistema operativo.

**Solución:**

- Actualizar a exacqVision Web Service, versión 20.06.2.0 o superior;
- actualizar a exacqVision Enterprise Manager, versión 20.06.3.0 o superior.

**Detalle:**

El *software* no verifica la firma criptográfica de los datos, lo que podría permitir a un atacante con privilegios administrativos descargar y abrir un archivo malicioso para ejecutar comandos del sistema operativo. Se ha reservado el identificador CVE-2020-9047 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

# Múltiples vulnerabilidades en varios productos de Mitsubishi Electric

**Fecha de publicación:** 19/06/2020

**Importancia:** Crítica

**Recursos afectados:**

- MC Works64, versiones 4.02C (10.95.208.31) y anteriores;
- MC Works32, versión 3.00A (9.50.255.02).

**Descripción:**

Varios investigadores han reportado 5 vulnerabilidades a ICONICS, una compañía del grupo Mitsubishi Electric, una con severidad crítica y 4 altas, de tipo escritura fuera de límites, deserialización de información no confiable e inyección de código.

**Solución:**

Mitsubishi Electric recomienda actualizar a la última versión del *software* disponible.

**Detalle:**

- Un paquete de comunicación, especialmente diseñado, enviado a alguno de los productos afectados, podría causar una condición de denegación de servicio (DoS) o permitir la ejecución remota de código. Se ha reservado el identificador CVE-2020-12011 para esta vulnerabilidad.
- Un paquete de comunicación, especialmente diseñado, enviado a los servicios de la plataforma MC Works64 afectada, podría causar una condición de denegación de servicio (DoS) debido a una deserialización incorrecta. Se ha reservado el identificador CVE-2020-12015 para esta vulnerabilidad.
- Un paquete de comunicación, especialmente diseñado, enviado a la función Workbench Pack & Go del producto afectad MC Works64, podría permitir la ejecución remota de código debido a una deserialización incorrecta. Se ha reservado el identificador CVE-2020-12009 para esta vulnerabilidad.
- Un mensaje, especialmente diseñado, enviado desde una función de cliente personalizada que interactúa con el servidor MC Works64 GridWorX afectado, podría permitir la ejecución de ciertos comandos SQL arbitrarios de forma remota y revelar datos internos, permitiendo la modificación de esos datos. Se ha reservado el identificador CVE-2020-12013 para esta vulnerabilidad.
- Un paquete de comunicación, especialmente diseñado, enviado al servidor FrameWorX del producto afectado MC Works64, podría permitir la ejecución remota de código y causar una condición de denegación de servicio (DoS) debido una deserialización inadecuada. Se ha reservado el identificador CVE-2020-12007 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

# Vulnerabilidades en Iconics Genesis32 y Genesis64

**Fecha de publicación:** 19/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Los productos que utilizan GenBroker64, Platform Services, Workbench, FrameWorX Server con versión 10.96 o anteriores son:

- GENESIS64,
- Hyper historiador,
- AnalytiX,
- MobileHMI.

Los productos con GenBroker32 versión v9.5 y anteriores son:

- GENESIS32,
- BizViz.

**Descripción:**

Investigadores de las empresas Claroty, Flashback, Incite y el Laboratorio Nacional Oak Ridge han descubierto diferentes vulnerabilidades en los productos de Iconics, que permitirían inyecciones remotas de código o ataques de denegación de servicio.

**Solución:**

Iconics lanzará las versiones 10.96, 10.95.5 y 10.95.2 para Genesis64 que corrigen estas vulnerabilidades, y las versiones 9.4 y 9.5 para Genesis32.

Para más información, se recomienda acudir a la página web de Iconics.

**Detalle:**

Las vulnerabilidades encontradas en los productos de Iconics podrían permitir ataques con escritura fuera de los límites, inyecciones de código o deserialización de datos no confiables.

La vulnerabilidad con mayor severidad es de carácter crítico y permitiría que un cliente WCF, especialmente diseñado, pudiera ejecutar comandos SQL arbitrarios de forma remota en el servidor Genesis64 FrameWorX.

Los identificadores asignados a estas vulnerabilidades son: CVE-2020-12011, CVE-2020-12015, CVE-2020-12009, CVE-2020-12013 y CVE-2020-12007.

**Etiquetas:** Actualización, Infraestructuras críticas, SCADA, Vulnerabilidad

# Múltiples vulnerabilidades en BIOTRONIK CardioMessenger II

**Fecha de publicación:** 19/06/2020

**Importancia:** Media

**Recursos afectados:**

- CardioMessenger II-S T-Line T4APP 2.20;
- CardioMessenger II-S GSM T4APP 2.20.

**Descripción:**

Múltiples vulnerabilidades podrían permitir a un atacante obtener datos confidenciales, obtener datos médicos transmitidos de dispositivos cardíacos implantados con el número de serie del implante, afectar a la funcionalidad del producto Cardio Messenger II o influir en las comunicaciones entre la Unidad HMU y la APN.

**Solución:**

BIOTRONIK informa que no emitirán una actualización de seguridad del producto, sin embargo ha implementado controles adicionales para reducir el riesgo de explotación y prevenir los riesgos de seguridad del paciente. Recomienda a los usuarios que tomen las siguientes medidas defensivas para minimizar el riesgo de explotación de estas vulnerabilidades:

- Mantener un buen control físico sobre las unidades de monitoreo en el hogar.
- Utilizar solo unidades de monitorización en el hogar que hayan sido obtenidas directamente de un proveedor de atención médica de confianza o un representante de BIOTRONIK para garantizar la integridad del sistema.
- Informar de cualquier comportamiento relacionado con estos productos a su proveedor de atención médica o un representante de BIOTRONIK.

**Detalle:**

- Los productos afectados no imponen correctamente la autenticación mutua con la infraestructura de comunicación remota de BIOTRONIK. Se ha reservado el identificador CVE-2019-18246 para esta vulnerabilidad.
- Los productos afectados transmiten credenciales en texto claro antes de cambiar a un canal de comunicación cifrado. Un atacante podría revelar las credenciales del cliente del producto para conectarse a la infraestructura de comunicación remota de BIOTRONIK. Se ha reservado el identificador CVE-2019-18248 para esta vulnerabilidad.
- Los productos afectados permiten la reutilización de credenciales para múltiples propósitos de autenticación. Un atacante con acceso adyacente al CardioMessenger podría revelar las credenciales utilizadas para conectarse a la infraestructura de comunicación remota de BIOTRONIK. Se ha reservado el identificador CVE-2019-18252 para esta vulnerabilidad.
- Los productos afectados no cifran información confidencial, mientras están en reposo. Un atacante con acceso físico al CardioMessenger podría obtener datos de mediciones médicas y el número de serie del dispositivo cardíaco implantado con el que está emparejado el CardioMessenger. Se ha reservado el identificador CVE-2019-18254 para esta vulnerabilidad.
- Los productos afectados utilizan credenciales individuales por dispositivo que se almacenan en un formato recuperable. Un atacante con acceso físico al CardioMessenger podría usar estas credenciales para la autenticación de red y descifrado de datos locales en tránsito. Se ha reservado el identificador CVE-2019-18256 para esta vulnerabilidad.

**Etiquetas:** Infraestructuras críticas, Sanidad, Vulnerabilidad

# Múltiples vulnerabilidades en Rockwell Automation FactoryTalk

**Fecha de publicación:** 19/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Se encuentran afectados por estas vulnerabilidades todas las versiones de FactoryTalk View SE y todas las versiones de FactoryTalk Services Platform.

**Descripción:**

Rockwell Automation, junto con Trend Micro's Zero Day Initiative, han publicado 5 vulnerabilidades, una de severidad crítica, 3 altas y una media, que permitirían que un atacante autenticado remoto manipule los datos de los dispositivos afectados, o que ejecute objetos COM remotos con privilegios elevados.

**Solución:**

Para FactoryTalk View SE se recomienda instalar los parches 1126289 y 1126289. Antes de instalar dichos parches se debe aplicar el parche acumulativo 1066644 - Parche Roll-up para CPR9 SRx del 6 de abril de 2020.

Rockwell Automation recomienda también para FactoryTalk View SE habilitar las funciones de seguridad integradas, siguiendo la guía de los artículos 109056 y 1126943 de su base de conocimiento para configurar IPSec y / o HTTP.

En el caso de FactoryTalk Services Platform se recomienda utilizar el artículo 25612 de la base de conocimientos de Rockwell, para determinar si este producto está instalado. En cuyo caso se deben implementar una estrategia de comunicación segura como la indicada en el artículo 109056 de la base de conocimientos.

**Detalle:**

Las vulnerabilidades encontradas en los productos de Rockwell Automation podrían permitir a un atacante acceder a información confidencial o no autorizada, realizar operaciones no permitidas dentro de los límites de un buffer de memoria, o modificar los permisos, controles y privilegios de acceso.

La vulnerabilidad más crítica de las encontradas (CVE-2020-12029) se produce al no validar correctamente el nombre de archivos dentro de un directorio del proyecto, pudiendo un atacante remoto no autenticado ejecutar un archivo diseñado y provocar una ejecución remota de código (RCE).

Los identificadores reservados a estas vulnerabilidades son CVE-2020-12029, CVE-2020-12031, CVE-2020-12028, CVE-2020-12027 y CVE-2020-12033.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Validación incorrecta de datos de entrada en Perseus A500 de Dräger

**Fecha de publicación:** 19/06/2020

**Importancia:** Media

**Recursos afectados:**

DrÃ¤ger Perseus A500, versiones de *software* desde la 2.00 hasta la 2.02.

**Descripción:**

Se ha publicado una vulnerabilidad del tipo validación inadecuada de los datos de entrada en DrÃ¤ger Perseus A500.

**Solución:**

Actualizar a la versión de *software* 2.03.

**Detalle:**

El producto afectado no valida correctamente ciertos datos específicamente diseñados que van a través de la interfaz Medibus. Esto podría permitir que la visualización de las curvas se retrase y, en última instancia, puede realizarse un inicio en caliente. Cuando se utilizan modos de ventilación controlados, un arranque en caliente hace que la presión de ventilación caiga hasta el nivel ambiente, lo que podría provocar un deterioro de la condición del paciente.

**Etiquetas:** Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

# Múltiples vulnerabilidades en varios productos de Baxter

**Fecha de publicación:** 19/06/2020

**Importancia:** Alta

**Recursos afectados:**

- ExactaMix EM2400, versiones 1.10, 1.11, 1.13 y 1.14;
- ExactaMix EM1200, versiones 1.1, 1.2, 1.4 y 1.5;
- PrismaFlex, todas las versiones;
- PrisMax, todas las versiones anteriores a 3.x;
- Phoenix Hemodialysis Delivery System SW, versiones 3.36 y 3.40.

**Descripción:**

Baxter ha reportado 11 vulnerabilidades a CISA, 6 con severidad alta y 5 medias, de tipo uso de credenciales en texto claro, transmisión de información sensible en texto claro, falta de cifrado de información sensible, control de acceso inadecuado, exposición de recursos a usuarios inadecuados, validación incorrecta de datos de entrada y autenticación inadecuada.

**Solución:**

- Los usuarios de ExactaMix EM 2400, versiones 1.10 y 1.11, y de ExactaMix EM1200, versiones 1.1 y 1.2, deben actualizar a ExactaMix 1.4 (EM1200) y ExactaMix 1.13 (EM2400);
- actualizar PrismaFlex a la versión 8.2x o posteriores;
- actualizar PrisMax a PrisMaxv3 con DCM (*Digital Communication Module*);
- a mayores, Baxter recomienda aplicar a todos sus usuarios las medidas de mitigación especificadas en sus respectivos avisos.

**Detalle:**

- El uso de credenciales de cuenta administrativa en claro permitiría a un atacante con acceso no autorizado a los recursos del sistema, incluido el acceso para ejecutar software o para ver/modificar archivos, directorios o la configuración del sistema, consultar datos confidenciales, incluida la PHI. Se ha reservado el identificador CVE-2020-12016 para esta vulnerabilidad.
- La utilización de mensajes de texto sin formato para comunicar información de pedidos, permitiría que un atacante accediese a la red y visualizase datos confidenciales, incluida la PHI. Se ha reservado el identificador CVE-2020-12008 para esta vulnerabilidad.
- El almacenamiento de datos del dispositivo con información confidencial en una base de datos sin cifrar, podría permitir que un atacante con acceso a la red vea o modifique datos confidenciales, incluida la PHI. Se ha reservado el identificador CVE-2020-12032 para esta vulnerabilidad.
- La validación incorrecta de datos de entrada a través del puerto SMBv1 podría afectar al flujo de control o al flujo de datos de un sistema, lo que permitiría a un atacante remoto obtener acceso no autorizado a información confidencial, crear condiciones de denegación de servicio (DoS) o ejecutar código arbitrario. Se ha asignado el identificador CVE-2017-0143 para esta vulnerabilidad.
- Los dispositivos afectados no requieren autenticación cuando se configuran para enviar datos de tratamiento a un sistema PDMS o EMR. Esto podría permitir a un atacante modificar la información del estado del tratamiento. Se ha reservado el identificador CVE-2020-12035 para esta vulnerabilidad.
- Un atacante con acceso a la red podría observar el tratamiento sensible y los datos de prescripción enviados entre el sistema Phoenix y la herramienta Exalis debido a la imposibilidad de cifrar los datos en tránsito, por ejemplo con TLS/SSL. Se ha reservado el identificador CVE-2020-12048 para esta vulnerabilidad.

Para las vulnerabilidades de severidad media, se han reservado los identificadores CVE-2020-12012, CVE-2020-12024, CVE-2020-12020, CVE-2020-12036 y CVE-2020-12037.

**Etiquetas:** Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

---

# Vulnerabilidades de transmisión de texto en claro de información sensible en múltiples productos de Honeywell

**Fecha de publicación:** 25/06/2020

**Importancia:** Media

**Recursos afectados:**

- ControlEdge PLC, versiones R130.2, R140, R150 y R151;
- ControlEdge RTU, versiones R101, R110, R140, R150 y R151.

**Descripción:**

Nikolay Sklyarenko, de Kaspersky, ha reportado 2 vulnerabilidades a CISA, ambas de severidad media y de tipo transmisión de texto en claro de información sensible.

**Solución:**

Honeywell ha proporcionado información detallada para mitigar la comunicación insegura en Control Edge PLC y RTU, a través del documento SN2020-04-17-01-ConotrolEdge-PLC-and- and-RTU-Secure-Communication.

**Detalle:**

- El dispositivo afectado expone contraseñas sin cifrar en la red. Se ha reservado el identificador CVE-2020-10628 para esta vulnerabilidad.
- El producto afectado expone un *token* de sesión en la red. Se ha reservado el identificador CVE-2020-10624 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Vulnerabilidad en productos Mitsubishi Electric

**Fecha de publicación:** 25/06/2020

**Importancia:** Crítica

**Recursos afectados:**

Todas las versiones de los módulos CPU en las series MELSEC iQ-R, iQ-F, Q, L y FX.

**Descripción:**

Shunkai Zhu, Rongkuan Ma y Peng Cheng, de NESC Lab, han reportado esta vulnerabilidad a Mitsubishi Electric que podría permitir a un atacante interceptar o manipular los datos de las comunicaciones, realizar operaciones no autorizadas o llevar a cabo ataques de denegación de servicio (DoS).

**Solución:**

Mitsubishi Electric recomienda cifrar las comunicaciones mediante el uso de una VPN para mitigar el impacto de esta vulnerabilidad.

**Detalle:**

Una vulnerabilidad debida a la comunicación en texto claro entre los módulos de CPU de las series iQ-R, iQ-F, Q, L y FX de Mitsubishi Electric MELSEC, y los módulos de CPU de las series GX Works3/GX Works2, podría permitir a un atacante interceptar o manipular los datos de las comunicaciones, realizar operaciones no autorizadas o llevar a cabo ataques de denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-14476 para esta vulnerabilidad.

**Etiquetas:** Infraestructuras críticas, Vulnerabilidad

---

# Vulnerabilidades en múltiples robots industriales

**Fecha de publicación:** 25/06/2020

**Importancia:** Crítica

**Recursos afectados:**

- MiR100, versiones 2.8.1.1 y anteriores;
- MiR200;
- MiR250;
- MiR500;
- MiR1000;
- ER200;

- ER-Lite;
- ER-Flex;
- ER-One;
- UVD.

**Descripción:**

Diversos investigadores de Alias Robotics y Joanneum Research han reportado 14 vulnerabilidades, 7 de severidad crítica, 5 altas y 2 medias, que afectan a varios productos de Mobile Industrial Robots A/S, EasyRobotics, Enabled Robotics y UVD Robots.

**Solución:**

Actualmente no hay actualizaciones que solucionen las vulnerabilidades.

**Detalle:**

Un atacante que aproveche las vulnerabilidades descritas en este aviso podría realizar las siguientes acciones:

- uso de credenciales en texto claro,
- exposición de recursos en un entorno inapropiado,
- falta de autenticación para función crítica,
- falta de cifrado de información sensible,
- exposición de información sensible a un usuario no autorizado,
- cifrado débil para contraseñas,
- desbordamiento de búfer de enteros,
- validación incorrecta de datos de entrada,
- fallo en la gestión de un elemento incompleto,
- permisos por defecto incorrectos,
- confianza en la seguridad a través de la falta de información,
- control de acceso inadecuado.

Las vulnerabilidades con severidad crítica se describen a continuación:

- Se puede acceder al panel de control de varios productos de MiR (Mobile Industrial Robots) utilizando una dirección IP en texto claro, lo que permitiría a un atacante tomar el control del robot de forma remota, utilizar las interfaces de usuario predeterminadas que MiR haya creado, borrar la autenticación y enviar solicitudes de red directamente. Se ha asignado el identificador CVE-2020-10270 para esta vulnerabilidad.
- La contraseña para el PLC de seguridad es la predeterminada, lo que permitiría que un programa manipulado se cargue en dicho PLC, deshabilitando la parada de emergencia en caso de que un objeto esté demasiado cerca del robot. La configuración del escáner láser también podría verse afectada. Se ha asignado el identificador CVE-2020-10276 para esta vulnerabilidad.
- Los tokens de acceso para la API REST se derivan directamente de las credenciales predeterminadas disponibles públicamente para la interfaz web. Un atacante no autorizado dentro de la red podría usar esas credenciales para calcular el token e interactuar con la API REST para filtrar, añadir o eliminar datos. Se ha asignado el identificador CVE-2020-10275 para esta vulnerabilidad.
- Algunos productos de la flota de MiR están preconfigurados en modo WiFi Master (Access Point), con unas credenciales (SSID y contraseña) bien conocidas y ampliamente difundidas, incluyendo en guías de usuario y manuales antiguos. Se ha asignado el identificador CVE-2020-10269 para esta vulnerabilidad.
- Algunos robots de MiR usan los paquetes predeterminados del ROS (Robot Operating System) que exponen el gráfico computacional sin ningún tipo de autenticación. Esto permitiría a los atacantes con acceso a las redes inalámbricas y cableadas internas tomar el control del robot sin problemas. En combinación con las vulnerabilidades CVE-2020-10269 y CVE-2020-10271, este fallo permite que los actores maliciosos comanden el robot a su antojo. Se ha asignado el identificador CVE-2020-10272 para esta vulnerabilidad.
- Varios robots de MiR usan los paquetes predeterminados del ROS (Robot Operating System) que exponen el gráfico computacional a todas las interfaces de red, inalámbricas y cableadas. En combinación con otros defectos como CVE-2020-10269, el gráfico de cálculo también se puede obtener e interactuar desde redes inalámbricas. Esto permite que un operador malintencionado tome el control de la lógica ROS y, en consecuencia, del robot completo. Se ha asignado el identificador CVE-2020-10271 para esta vulnerabilidad.
- Los controladores de robot MiR (unidad central de cómputo) utilizan Ubuntu 16.04.2 como sistema operativo, que contiene fallos de seguridad, como una forma para que los usuarios escalen su acceso más allá de lo que se les otorgó, a través de la creación de archivos, condiciones de carrera de acceso, configuraciones inseguras del directorio de inicio y valores predeterminados que facilitan los ataques de Denegación de Servicio (DoS). Se ha asignado el identificador CVE-2020-10279 a esta vulnerabilidad.

Para las vulnerabilidades de severidad alta y media se han asignado los identificadores: CVE-2020-10273, CVE-2020-10274, CVE-2017-18255, CVE-2017-7184, CVE-2020-10280, CVE-2020-10277 y CVE-2020-10278.

**Etiquetas:** Vulnerabilidad

---

# Múltiples vulnerabilidades en controladores de luz ENTTEC

**Fecha de publicación:** 26/06/2020

**Importancia:** Alta

**Recursos afectados:**

Estas vulnerabilidades afectan al firmware versión 70044_actualización_05032019-482 y anteriores, para los siguientes productos:

- Datagate Mk2,
- Storm 24,
- Pixelator,
- E-Streamer Mk2.

**Descripción:**

Se han publicado múltiples vulnerabilidades presentes en controladores de luz que podrían permitir a un atacante obtener acceso SSH/SCP no autorizado a los dispositivos, inyectar código malicioso, ejecutar comandos con privilegios de *root* o leer, escribir y ejecutar archivos en los directorios del sistema como cualquier otro usuario.

**Solución:**

ENTTEC aún no ha lanzado ninguna actualización. Recomienda que los dispositivos se ubiquen detrás de los *firewalls* y controles de red apropiados, y que no sean accesibles desde Internet.

**Detalle:**

- La existencia de contraseñas embebidas para el acceso remoto SSH y SCP como usuario *root*. Se ha asignado el identificador CVE-2019-12776 para esta vulnerabilidad.
- Varias vulnerabilidades de XSS almacenado, en el *software* de configuración web Datagate Mk2 de ENTTEC, podrían permitir a un atacante no autenticado inyectar código malicioso directamente en la aplicación. Se ha asignado el identificador CVE-2019-12774 para esta vulnerabilidad.
- Los controladores de luz permiten acceso de alto privilegio como *root* a través de la capacidad de sudo sin requerir un control de acceso apropiado. Se ha asignado el identificador CVE-2019-12775 para esta vulnerabilidad.
- El sistema remplaza los permisos del sistema operativo subyacente con permisos altamente inseguros de lectura, escritura y ejecución para todos los usuarios. Se ha asignado el identificador CVE-2019-12777 para esta vulnerabilidad.

**Etiquetas:** Infraestructuras críticas, Vulnerabilidad

---

# Múltiples vulnerabilidades en varios productos de Rockwell Automation

**Fecha de publicación:** 26/06/2020

**Importancia:** Alta

**Recursos afectados:**

- FactoryTalk Services Platform, versiones 6.11.00 y anteriores;
- FactoryTalk View SE, versiones:
  - 9.0 y anteriores;
  - 10.0.

**Descripción:**

Applied Risk, junto con Ilya Karpov y Evgeny Druzhinin de ScadaX Security, han reportado 3 vulnerabilidades a Rockwell Automation, todas de severidad alta, de tipo restricción inadecuada de referencia a XXE (*XML External Entity*), almacenamiento de información sensible en texto claro y cifrado de contraseña débil.

**Solución:**

- Seguir las instrucciones de 1092746 para actualizar FactoryTalk Services Platform;
- se recomienda a los usuarios de las versiones afectadas de DeskLock proporcionadas con FactoryTalk View SE que actualicen a una versión de *software* 10.0 o posterior.

**Detalle:**

- Un atacante remoto, no autenticado, podría usar un ataque de entidad externa XML (XXE) para explotar archivos XML mal configurados, logrando acceder a contenido local o remoto. Esto podría causar una condición de denegación de servicio (DoS) y permitiría al atacante leer arbitrariamente cualquier archivo local a través de servicios a nivel de sistema. Se ha reservado el identificador CVE-2020-14478 para esta vulnerabilidad.
- Debido a que las credenciales se almacenan en texto sin formato en la RAM, un atacante autenticado, local, podría obtener acceso a ciertas credenciales, incluidas las de inicio de sesión de Windows. Se ha reservado el identificador CVE-2020-14480 para esta vulnerabilidad.
- La herramienta DeskLock, proporcionada con FactoryTalk View SE, utiliza un algoritmo de cifrado débil que podría permitir que un atacante autenticado, local, descifre las credenciales del usuario, incluido el usuario de Windows o las contraseñas de Windows DeskLock. Si el usuario comprometido tiene una cuenta administrativa, el atacante podría obtener acceso completo al sistema operativo del usuario y a ciertos componentes de FactoryTalk View SE. Se ha reservado el identificador CVE-2020-14481 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Vulnerabilidad

---

# Fallos de autenticación en Philips Ultrasound Systems

**Fecha de publicación:** 26/06/2020

**Importancia:** Baja

**Recursos afectados:**

- Ultrasonido ClearVue, versiones 3.2 y anteriores.
- Ultrasonido CX, versiones 5.0.2 y anteriores.
- Ultrasonido EPIQ / Affiniti, versiones VM5.0 y anteriores.
- Ultrasonido Sparq, versiones 3.0.2 y anteriores.
- Ultrasonido Xperius, todas las versiones.

**Descripción:**

Philips ha informado de una vulnerabilidad en sus productos Ultrasound Systems que podría permitir que un atacante, no autenticado, vea o modifique información del sistema.

**Solución:**

Se recomienda instalar la versión de abril 2020 de Ultrasound EPIQ / Affiniti Versión VM6.0. Philips recomienda además a los usuarios de sistemas Ultrasound EPIQ / Affiniti contactar con su equipo de soporte regional.

Para otros productos está previsto solucionar esta vulnerabilidad en las siguientes versiones:

- Ultrasound ClearVue versión 3.3, prevista para el cuatro trimestre de 2020.
- Ultrasound CX versión 5.0.3, prevista para el cuatro trimestre de 2020.
- Ultrasound Sparq versión 3.0.3, prevista para el cuatro trimestre de 2020.

Philips recomienda además garantizar que los proveedores de servicios que usan los dispositivos puedan tener disponibilidad de los dispositivos durante las tareas de operación del servicio.

Se recomienda contactar con el servicio técnico de Philips o con su equipo de soporte regional.

**Detalle:**

La vulnerabilidad detectada en los productos Philips Ultrasound Systems permitiría a un atacante usar una ruta o canal alternativo que no necesite autenticación de inicio de sesión, para ver o modificar información. Se ha reservado el identificador CVE-2020-14477 para esta vulnerabilidad.

**Etiquetas:** Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad