



Centro de  
**Ciberseguridad Industrial**

# Vulnerabilidades ICS Termómetro CCI 2021- 5

📍 PASEO DE LAS DELICIAS, 30 - 2º

28045 MADRID

☎ +34 910 910 751

✉ [INFO@CCI-ES.ORG](mailto:INFO@CCI-ES.ORG)

🌐 [WWW.CCI-ES.ORG](http://WWW.CCI-ES.ORG)

**B** [BLOG.CCI-ES.ORG](http://BLOG.CCI-ES.ORG)

🐦 [@INFO\\_CCI](https://twitter.com/INFO_CCI)



# Tabla de contenido

<b>Introducción .....</b>	<b>4</b>
Novedades 2021.....	4
<b>Fabricantes y debilidades ICS .....</b>	<b>5</b>
Nuevos fabricantes.....	5
Nuevas debilidades .....	5
Nuevas alertas .....	6
<b>Mapa de riesgo .....</b>	<b>7</b>
Cambios en el riesgo de fabricante.....	7
<b>ANEXO – I: Cálculo del mapa de riesgo .....</b>	<b>8</b>
<b>ANEXO II – Vulnerabilidades publicadas por el NIST desde el último termómetro CCI....</b>	<b>9</b>



Profesional de la Ciberseguridad industrial desde hace más de diez años en distintas empresas como Schneider Electric, S21sec, EY, SecurityMatters, Forescout, Telefónica y actualmente en TITANIUM Industrial Security.

Miembro activo del ecosistema del Centro de Ciberseguridad Industrial (CCI) desde 2013, profesional Nivel Negro y participando como autor y revisor de distintos estudios y documentos realizados por este.



## Introducción

Desde la publicación del cuaderno “Una década de vulnerabilidades ICS” el 4 de mayo de 2020, se han seguido publicando nuevas vulnerabilidades sobre sistemas ICS, lo que ha hecho variar la exposición al riesgo de los fabricantes recogidos en dicho cuaderno.

Desde el CCI queremos mantener actualizada esta información para proporcionar una visión de la evolución de estas vulnerabilidades para que el ecosistema pueda utilizarlas cómo precise en una publicación que denominaremos **Termómetro de vulnerabilidades ICS del CCI**.

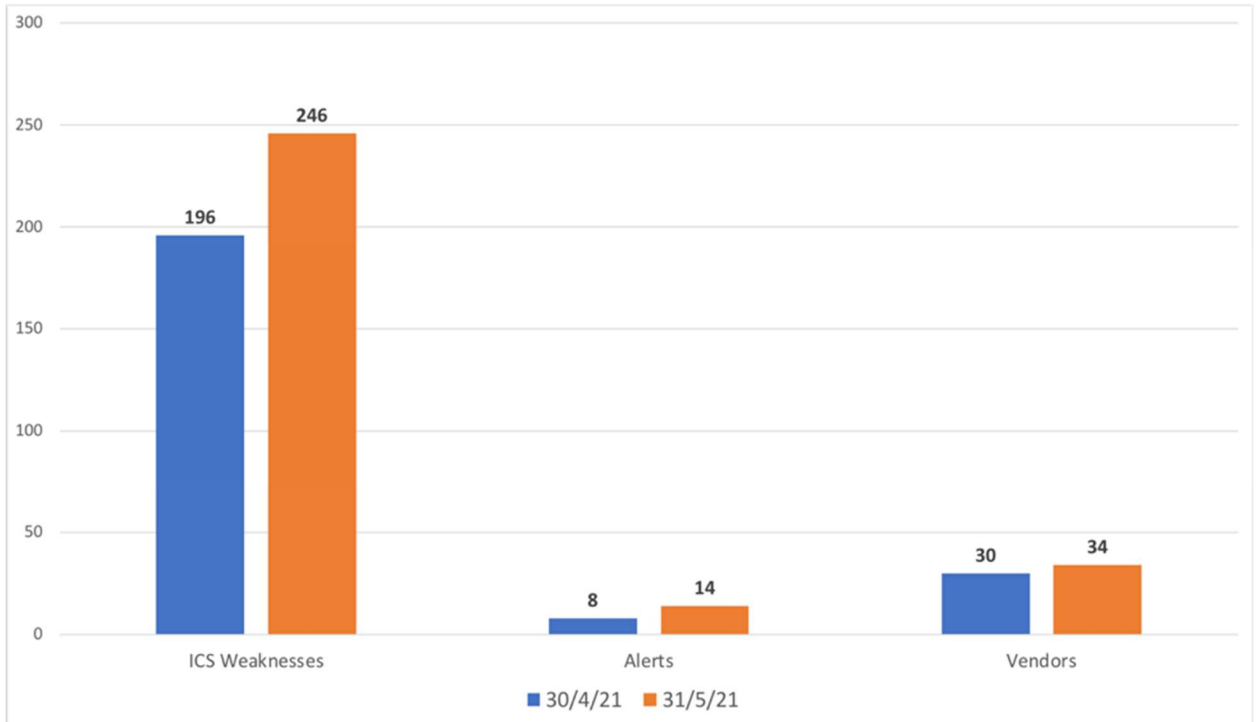
En cada actualización publicaremos:

- **Evolución del número de fabricantes de sistemas de control incluidos en el termómetro para el periodo en curso**
- **Evolución de vulnerabilidades y alertas de los fabricantes de control incluidos en el termómetro**
- **El mapa de calor de exposición al riesgo de los fabricantes, actualizado a fecha de publicación.**
- **Comentarios acerca de la evolución del mapa de riesgo.**

## Novedades 2021

Para adaptarnos a la creciente casuística de vulnerabilidades públicas que afectan a varios fabricantes, en el año 2021 se aplicará un nuevo criterio, publicando cada uno de los fabricantes afectados por esta única vulnerabilidad (CVE). Para ser coherentes con este nuevo acercamiento, en 2021 hablaremos de “Debilidades ICS” (ICS Weaknesses) para dar cabida a estas vulnerabilidades multifabricante.

## Fabricantes y debilidades ICS



## Nuevos fabricantes

En esta edición del termómetro CCI, se incluyen 5 nuevos fabricantes y su número pasa a **35**.

Riesgo Bajo	Riesgo Medio	Riesgo Alto	Riesgo Muy Alto
Beckhoff SearchBlox Wago	Zebra Industrial Motorola Solutions	N/A	N/A

La vulnerabilidad CVE-2021-32089, afecta a un producto originalmente de Motorola (LECTOR FIJO DE RFID FX9600), que posteriormente fue adquirido por Zebra Industrial. En la actualidad no cuenta con soporte del fabricante.

En el caso de Beckhoff, las vulnerabilidades afectan a su producto TwinCAT OPC UA Server, y Wago registra 8 vulnerabilidades que afectan a muchos de sus switches industriales y a sus PLCs (Wago PFC200).





## Nuevas debilidades

El número de vulnerabilidades ICS publicadas por el NIST desde la última actualización es de **58**.

Dos fabricantes acumulan casi el 50% de este número:

- **Mikrotik** con **13** debilidades publicadas en mayo de 2021 asociadas a su sistema operativo (RouterOs), es el fabricante que registra más debilidades
- **Siemens** con **12 CVEs** publicadas en mayo (una de ellas considerada alerta) y que sigue encabezando el mapa cualitativo de riesgo. Es de destacar que, a mayo de 2021, se han publicado casi tantas vulnerabilidades (**93**) que en todo el año 2020 (**95**).

**Moxa** registra **9** debilidades, de las cuales **4** generan alertas. Todas estas vulnerabilidades publicadas, se concentran en dos familias de productos: Switches y Cámaras IP utilizadas en el sector ferroviario. Este último caso se comentará en detalle en el punto siguiente.

**Wago** sufre **8** nuevas debilidades que afectan a un gran número de sus switches de red, por lo que su exposición al riesgo aumenta bastante, dado que su CVSS V2 acumulado en los últimos 10 años llega a **6.4**.

**Emerson** registra **5** debilidades en el interfaz web de su producto **Rosemount X-STREAM Gas Analyzer**, llegando a un CVSS V2 medio de **6.3** en los últimos 10 años.

**Zebra Industrial / Motorola Solutions** registran 1 única vulnerabilidad que comento por tratarse de un lector RFID Industrial fuera de soporte del fabricante, por lo que supone una amenaza difícil de mitigar .

## Nuevas alertas

Este mes, el **NIST** ha publicado **6 nuevas alertas** de fabricante. Recordamos que se clasifican cómo alertas dado que la explotación de la vulnerabilidad presenta una complejidad baja, tiene cómo vector de acceso la red y puede causar una total pérdida de servicio. (Según la clasificación **CVSS V2**, para permitir la clasificación histórica de debilidades en productos más antiguos).

**4** de estas alertas se asocian a un producto de **Moxa** (Camera VPort 06EC-2V). He estudiado estas debilidades más en detalle por tratarse de un producto certificado para su uso embarcado en trenes y relacionado con la seguridad física de las personas. En breve publicaré un resumen de esto a título personal.



Moxa Camera VPort 06EC-2V

CVE	Date published	CVSS	Warning	Description
<a href="#">CVE-2021-25848</a>	2021-05-10	8.5		Improper validation of the length field of LLDP-MED TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows information disclosure to attackers due to using fixed loop counter variable without checking the actual available length via a crafted lldp packet.
<a href="#">CVE-2021-25847</a>	2021-05-10	8.5		Improper validation of the length field of LLDP-MED TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows information disclosure to attackers due to controllable loop counter variable via a crafted lldp packet.
<a href="#">CVE-2021-25846</a>	2021-05-10	7.8		Improper validation of the ChassisID TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows attackers to cause a denial of service due to a negative number passed to the memcpy function via a crafted lldp packet.
<a href="#">CVE-2021-25849</a>	2021-05-10	7.8		An integer underflow was discovered in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, improper validation of the PortID TLV leads to Denial of Service via a crafted lldp packet.

**Advantech** también se ha recogido como alerta en esta edición, al haberse actualizado en mayo la información sobre una vulnerabilidad publicada en abril. (Recordemos que el termómetro del CCI no es un sistema de alerta temprana, sino una cualificación cualitativa de debilidades y fabricantes ICS).

CVE	Date published	CVSS	Warning	Description
<a href="#">CVE-2021-22669</a>	2021-04-26	9.0		Incorrect permissions are set to default on the 'Project Management' page of WebAccess/SCADA portal of WebAccess/SCADA Versions 9.0.1 and prior, which may allow a low-privileged user to update an administrator's password and login as an administrator to escalate privileges on the system.



La última alerta está relacionada con un producto de **Siemens** (SIMATIC NET CP 343-1) y su explotación puede llevar a una pérdida total del servicio.

CVE	Date published	CVSS	Warning	Description
<a href="#">CVE-2020-25242</a>	2021-05-12	7.8		A vulnerability has been identified in SIMATIC NET CP 343-1 Advanced (incl. SIPLUS variants) (All versions), SIMATIC NET CP 343-1 Lean (incl. SIPLUS variants) (All versions), SIMATIC NET CP 343-1 Standard (incl. SIPLUS variants) (All versions). Specially crafted packets sent to TCP port 102 could cause a Denial-of-Service condition on the affected devices. A cold restart might be necessary in order to recover.





# Mapa de riesgo

31 de mayo de 2021

	Mitsubishi Electric Panasonic			
Delta Electronics Motorola Solutions Pro-face Schneider Electric Wind River Zebra Industrial	Advantech Emerson Hilscher Moxa			
Belden Digi Eaton Fatek Fuji Electric Hirschmann Honeywell Kepware Omron PTC (ThingWorx) Rockwell Software Toolbox	GE Mikrotik			Siemens
ABB Beckhoff Philips ProSoft RuggedCom SearchBlox Tesla Wago				

## Cambios en el riesgo de fabricante

Las cuatro alertas publicadas sobre un producto de **Moxa** hacen que pase de un nivel de riesgo Medio a Medio+ y obtiene de esta manera un CVSS V2 medio de **6.2** en los últimos 10 años.

**Zebra Industrial/Motorola Solutions** ingresan directamente en el mapa con Riesgo Medio debido a la debilidad detectada sobre su lector RFID industrial.

Paradójicamente, **Mikrotik** disminuye su exposición al riesgo a pesar del alto número de vulnerabilidades publicadas en mayo sobre sus productos. obtiene un CVSS V2 medio de **5.7** en los últimos 10 años.

El resto de los fabricantes, incluido **Emerson**, mantienen su nivel en el mapa de calor cualitativo de exposición al riesgo.

## ANEXO – I: Cálculo del mapa de riesgo

Con objeto de mostrar de una manera gráfica y rápida la postura de cada fabricante en lo que se refiere al riesgo asociado a las vulnerabilidades publicadas, he seleccionado un formato gráfico muy común en la gestión de Riesgos: el mapa de calor.

Este diagrama presenta distintos colores para representar el riesgo asociado de manera cualitativa y en cuatro rangos: Bajo, Medio, Alto y Muy Alto.

				MUY ALTO
		ALTO		
	MEDIO			
BAJO				

La posición de cada fabricante dentro del mapa depende de los valores obtenidos en dos parámetros asociados con la **probabilidad** (Número de CVEs publicados) y el **impacto** de dichos CVEs (Valor medio de CVSS).

Para cada año, se ha calculado cada uno de estos valores entre 1 y 5.

- En el eje horizontal, se ha calculado el valor proporcional al número de CVEs publicados para ese fabricante en un año concreto en comparación con el fabricante con mayor número de CVEs.
- En el eje vertical se ha calculado el valor medio de CVSS de los CVEs publicados ese año y se ha dividido entre 2.

Para intentar dar una idea más cualitativa en lo que se refiere a la postura de cada fabricante, se han introducido dos correcciones en el cálculo:

- Si el fabricante tiene algún CVE ese año considerado como **Alerta** (Acceso por la red, complejidad baja e impacto completo en disponibilidad), se incrementa en una unidad el impacto (Eje vertical) y en una unidad la probabilidad (Eje horizontal). Esto se realiza para diferenciar a este fabricante de otros sin este tipo de CVEs y posicionarlo en una zona de mayor riesgo.
- De la misma manera, si un fabricante tiene algún CVE ese año con un valor CVSS de 10.0, se incrementa en una unidad la probabilidad (Eje horizontal). Esto se realiza para diferenciar a este fabricante de otros sin este tipo de CVEs y posicionarlo en una zona de mayor riesgo.

Se ha estudiado mediante distintas simulaciones que estas correcciones no suponen grandes alteraciones en la postura global del riesgo de ese fabricante y, sin embargo, presentan un diagnóstico cualitativo más ajustado.



## ANEXO II – Vulnerabilidades publicadas por el NIST desde el último termómetro CCI

CVE	Date published	CVSS	Warning	Description
CVE-2020-20266	2021-05-19	4.0		Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/dot1x process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).
CVE-2021-21000	2021-05-24	5.0		On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime.
CVE-2021-21001	2021-05-24	4.0		On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges.
CVE-2021-27459	2021-05-20	7.5		A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code.
CVE-2021-27467	2021-05-20	5.8		A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information.
CVE-2021-27461	2021-05-20	5.0		A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs.
CVE-2021-27463	2021-05-20	5.0		A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information.
CVE-2020-35580	2021-05-20	5.0		A local file inclusion vulnerability in the FileServlet in all SearchBlox before 9.2.2 allows remote, unauthenticated users to read arbitrary files from the operating system via a /searchblox/servlet/FileServlet?col=url= request. Additionally, this may be used to read the contents of the SearchBlox configuration file (e.g., searchblox/WEB-INF/config.xml), which contains both the Super Admin's API key and the base64 encoded SHA1 password hashes of other SearchBlox users.
CVE-2021-27465	2021-05-20	4.3		A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data.
CVE-2021-21000	2021-05-24	5.0		On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime.
CVE-2020-20227	2021-05-18	4.0		Mikrotik RouterOs stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/disk process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access.
CVE-2020-20246	2021-05-18	4.0		Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the mactel process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.
CVE-2020-20245	2021-05-18	4.0		Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the log process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.
CVE-2020-20236	2021-05-18	4.0		Mikrotik RouterOs 6.46.3 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service due to improper memory access.
CVE-2020-20214	2021-05-18	4.0		Mikrotik RouterOs 6.44.6 (long-term tree) suffers from an assertion failure vulnerability in the bttest process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.
CVE-2020-20222	2021-05-18	4.0		Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).
CVE-2020-20220	2021-05-18	4.0		Mikrotik RouterOs prior to stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/bfd process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).



CVE	Date published	CVSS	Warning	Description
CVE-2020-20253	2021-05-18	4.0		Mikrotik RouterOs before 6.47 (stable tree) suffers from a division by zero vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service due to a divide by zero error.
CVE-2021-27734	2021-05-17	7.5		Hirschmann HiOS 07.1.01, 07.1.02, and 08.1.00 through 08.5.xx and HiSecOS 03.3.00 through 03.5.01 allow remote attackers to change the credentials of existing users.
CVE-2020-27150	2021-05-14	5.0		In multiple versions of NPort IA5000A Series, the result of exporting a device's configuration contains the passwords of all users on the system and other sensitive data in the original form if "Pre-shared key" doesn't set.
CVE-2020-27185	2021-05-14	5.0		Cleartext transmission of sensitive information via Moxa Service in NPort IA5000A series serial devices. Successfully exploiting the vulnerability could enable attackers to read authentication data, device configuration, and other sensitive data transmitted over Moxa Service.
CVE-2020-27184	2021-05-14	4.3		The NPort IA5000A Series devices use Telnet as one of the network device management services. Telnet does not support the encryption of client-server communications, making it vulnerable to Man-in-the-Middle attacks.
CVE-2020-27149	2021-05-14	4.0		By exploiting a vulnerability in NPort IA5150A/IA5250A Series before version 1.5, a user with "Read Only" privilege level can send requests via the web console to have the device's configuration changed.
CVE-2021-20998	2021-05-13	7.5		In multiple managed switches by WAGO in different versions without authorization and with specially crafted packets it is possible to create users.
CVE-2021-27413	2021-05-13	6.8		Omron CX-One Versions 4.60 and prior, including CX-Server Versions 5.0.29.0 and prior, are vulnerable to a stack-based buffer overflow, which may allow an attacker to execute arbitrary code.
CVE-2021-20995	2021-05-13	5.0		In multiple managed switches by WAGO in different versions the webserver cookies of the web based UI contain user credentials.
CVE-2021-20993	2021-05-13	5.0		In multiple managed switches by WAGO in different versions the activated directory listing provides an attacker with the index of the resources located inside the directory.
CVE-2021-20996	2021-05-13	5.0		In multiple managed switches by WAGO in different versions special crafted requests can lead to cookies being transferred to third parties.
CVE-2021-20997	2021-05-13	5.0		In multiple managed switches by WAGO in different versions it is possible to read out the password hashes of all Web-based Management users.
CVE-2021-20988	2021-05-13	5.0		In Hilscher rxC RTOS versions prior to V2.1.14.1 the actual UDP packet length is not verified against the length indicated by the packet. This may lead to a denial of service of the affected device.
CVE-2020-12526	2021-05-13	5.0		TwinCAT OPC UA Server in versions up to 2.3.0.12 and IPC Diagnostics UA Server in versions up to 3.1.0.1 from Beckhoff Automation GmbH & Co. KG are vulnerable to denial of service attacks. The attacker needs to send several specifically crafted requests to the running OPC UA server. After some of these requests the OPC UA server is no longer responsive to any client. This is without effect to the real-time functionality of IPCs.
CVE-2021-20994	2021-05-13	4.3		In multiple managed switches by WAGO in different versions an attacker may trick a legitimate user to click a link to inject possible malicious code into the Web-Based Management.
CVE-2021-27384	2021-05-12	7.5		SmartVNC has an out-of-bounds memory access vulnerability in the device layout handler represented by a binary data stream on client side, which could result in code execution on the SIMATIC HMIs/WinCC Products SIMATIC HMI Comfort Outdoor Panels 7' and 15' (incl. SIPLUS variants), SIMATIC HMI Comfort Panels 4'to 22' (incl. SIPLUS variants), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900, and KTP900F, SIMATIC WinCC Runtime Advanced (All versions prior to v16 Update 4).
CVE-2020-28393	2021-05-12	7.1		An unauthenticated remote attacker could create a permanent denial-of-service condition by sending specially crafted OSPF packets. Successful exploitation requires OSPF to be enabled on an affected device on the SCALANCE XM-400, XR-500 (All versions prior to v6.4).
CVE-2021-27396	2021-05-12	6.8		A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V16.0.5). The PlantSimCore.dll library lacks proper validation of user-supplied data when parsing SPP files. This could result in a stack based buffer overflow, a different vulnerability than CVE-2021-27398. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13279)
CVE-2021-27398	2021-05-12	6.8		A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V16.0.5). The PlantSimCore.dll library lacks proper validation of user-supplied data when parsing SPP files. This could result in a stack based buffer overflow, a different vulnerability than CVE-2021-27396. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13290)
CVE-2021-27397	2021-05-12	6.8		A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V16.0.5). The PlantSimCore.dll library lacks proper validation of user-supplied data when parsing SPP files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13287)



CVE	Date published	CVSS	Warning	Description
CVE-2021-25661	2021-05-12	5.0		SmartVNC has an out-of-bounds memory access vulnerability that could be triggered on the client side when sending data from the server, which could result in a denial-of-service condition on the SIMATIC HMIs/WinCC Products SIMATIC HMI Comfort Outdoor Panels 7' and 15' (incl. SIPLUS variants), SIMATIC HMI Comfort Panels 4' to 22' (incl. SIPLUS variants), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900, and KTP900F, SIMATIC WinCC Runtime Advanced (All versions prior to v16 Update 4).
CVE-2021-27383	2021-05-12	5.0		SmartVNC has a heap allocation leak vulnerability in the server Tight encoder, which could result in a denial-of-service condition on the SIMATIC HMIs/WinCC Products SIMATIC HMI Comfort Outdoor Panels 7' and 15' (incl. SIPLUS variants), SIMATIC HMI Comfort Panels 4' to 22' (incl. SIPLUS variants), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900, and KTP900F, SIMATIC WinCC Runtime Advanced (All versions prior to v16 Update 4).
CVE-2021-25662	2021-05-12	5.0		SmartVNC client fails to handle an exception properly if the program execution process is modified after sending a packet from the server, which could result in a denial-of-service condition on the SIMATIC HMIs/WinCC Products SIMATIC HMI Comfort Outdoor Panels 7' and 15' (incl. SIPLUS variants), SIMATIC HMI Comfort Panels 4' to 22' (incl. SIPLUS variants), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900, and KTP900F, SIMATIC WinCC Runtime Advanced (All versions prior to v16 Update 4).
CVE-2021-25660	2021-05-12	5.0		A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 4). SmartVNC has an out-of-bounds memory access vulnerability that could be triggered on the server side when sending data from the client, which could result in a Denial-of-Service condition.
CVE-2021-27386	2021-05-12	5.0		A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Advanced (All versions < V16 Update 4). SmartVNC has a heap allocation leak vulnerability in the device layout handler on client side, which could result in a Denial-of-Service condition.
CVE-2021-27385	2021-05-12	5.0		A remote attacker could send specially crafted packets to a SmartVNC device layout handler on the client side, which could influence the number of resources consumed and result in a denial-of-service condition (infinite loop) on the SIMATIC HMIs/WinCC Products SIMATIC HMI Comfort Outdoor Panels 7' and 15' (incl. SIPLUS variants), SIMATIC HMI Comfort Panels 4' to 22' (incl. SIPLUS variants), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900, and KTP900F, SIMATIC WinCC Runtime Advanced (All versions prior to v16 Update 4).
CVE-2021-32089	2021-05-11	7.5		** UNSUPPORTED WHEN ASSIGNED ** An issue was discovered on Zebra (formerly Motorola Solutions) Fixed RFID Reader FX9500 devices. An unauthenticated attacker can upload arbitrary files to the filesystem that can then be accessed through the web interface. This can lead to information disclosure and code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2020-20265	2021-05-11	4.0		Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /ram/pckg/wireless/nova/bin/wireless process. An authenticated remote attacker can cause a Denial of Service due via a crafted packet.
CVE-2020-20267	2021-05-11	4.0		Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/resolver process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access.
CVE-2021-22672	2021-05-10	6.8		Delta Electronics' CNCSoft ScreenEditor in versions prior to v1.01.30 could allow the corruption of data, a denial-of-service condition, or code execution. The vulnerability may allow an attacker to remotely execute arbitrary code.
CVE-2021-25845	2021-05-10	5.0		Improper validation of the ChassisID TLV in userdisk/vport_Ildpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows attackers to cause a denial of service due to a NULL pointer dereference via a crafted Ildp packet.
CVE-2021-27437	2021-05-07	6.4		The affected product allows attackers to obtain sensitive information from the WISE-PaaS dashboard. The system contains a hard-coded administrator username and password that can be used to query Grafana APIs. Authentication is not required for exploitation on the WISE-PaaS/RMM (versions prior to 9.0.1).
CVE-2020-20218	2021-05-03	4.0		Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/traceroute process. An authenticated remote attacker can cause a Denial of Service due via the loop counter variable.
CVE-2020-20247	2021-05-03	4.0		Mikrotik RouterOs before 6.46.5 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/traceroute process. An authenticated remote attacker can cause a Denial of Service due via the loop counter variable.



CVE	Date published	CVSS	Warning	Description
CVE-2021-25848	2021-05-10	8.5		Improper validation of the length field of LLDP-MED TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows information disclosure to attackers due to using fixed loop counter variable without checking the actual available length via a crafted lldp packet.
CVE-2021-25847	2021-05-10	8.5		Improper validation of the length field of LLDP-MED TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows information disclosure to attackers due to controllable loop counter variable via a crafted lldp packet.
CVE-2021-25846	2021-05-10	7.8		Improper validation of the ChassisID TLV in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, allows attackers to cause a denial of service due to a negative number passed to the memcpy function via a crafted lldp packet.
CVE-2021-25849	2021-05-10	7.8		An integer underflow was discovered in userdisk/vport_lldpd in Moxa Camera VPort 06EC-2V Series, version 1.1, improper validation of the PortID TLV leads to Denial of Service via a crafted lldp packet.
CVE-2021-22669	2021-04-26	9.0		Incorrect permissions are set to default on the 'Project Management' page of WebAccess/SCADA portal of WebAccess/SCADA Versions 9.0.1 and prior, which may allow a low-privileged user to update an administrator's password and login as an administrator to escalate privileges on the system.
CVE-2020-25242	2021-05-12	7.8		A vulnerability has been identified in SIMATIC NET CP 343-1 Advanced (incl. SIPLUS variants) (All versions), SIMATIC NET CP 343-1 Lean (incl. SIPLUS variants) (All versions), SIMATIC NET CP 343-1 Standard (incl. SIPLUS variants) (All versions). Specially crafted packets sent to TCP port 102 could cause a Denial-of-Service condition on the affected devices. A cold restart might be necessary in order to recover.