Industrial Cybersecurity Center

ICS Vulnerabilities
CCI Thermometer
2021- 11

PASEO DE LAS DELICIAS, 30 - 2°
28045 MADRID
+34 910 910 751
INFO@CCI-ES.ORG
WWW.CCI-ES.ORG
BLOG.CCI-ES.ORG
@INFO_CCI

Table of contents

Industrial Cybersecurity professional for more than ten years in different companies such as Schneider Electric, S21sec, EY, SecurityMatters, Forescout, Telefonica and currently at TITANIUM Industrial Security.

Active member of the Industrial Cybersecurity Center's ecosystem since 2013, Black Level professional and participating as author and reviewer of different studies and documents carried out by it.

Introduction

Since the publication of the notebook "A decade of ICS vulnerabilities" on May 4, 2020, new vulnerabilities have been published on ICS systems, which has changed the exposure to risk of the manufacturers included in that notebook.

From the CCI we want to keep this information updated to provide a view of the evolution of these vulnerabilities so that the ecosystem can use them as necessary in a publication that we will call the CCI ICS Vulnerability Thermometer.

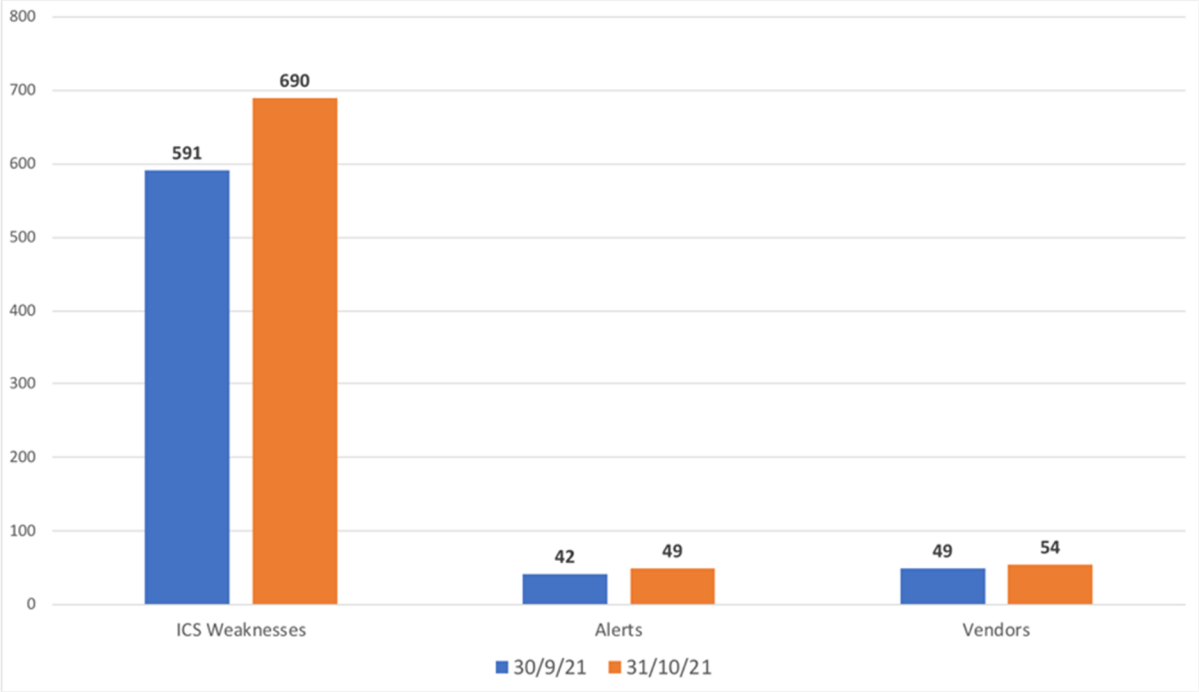
In each update we will publish:

- Evolution of the number of control manufacturers included in the thermometer for the current period.
- Evolution of vulnerabilities and alerts from control manufacturers included in the thermometer.
- The manufacturers heat exposure risk map updated as of publication date.
- Comments about the evolution of the risk map.

2021 Developments

To adapt to the growing casuistry of public vulnerabilities that affect various manufacturers, in 2021 a new criterion will be applied, publishing each of the manufacturers affected by this single vulnerability (CVE). To be consistent with this new approach, in 2021 we will speak of "ICS Weaknesses" to accommodate these multi-vendor vulnerabilities.

Manufacturers and ICS weaknesses



New manufacturers

In this edition of the CCI Thermometer, **2** new **manufacturers** are included, and their number increases to **56** in 2021:

Low Risk	Medium Risk	High Risk	Very High Risk
Azeotech OSIsoft	N/A	N/A	Dahua

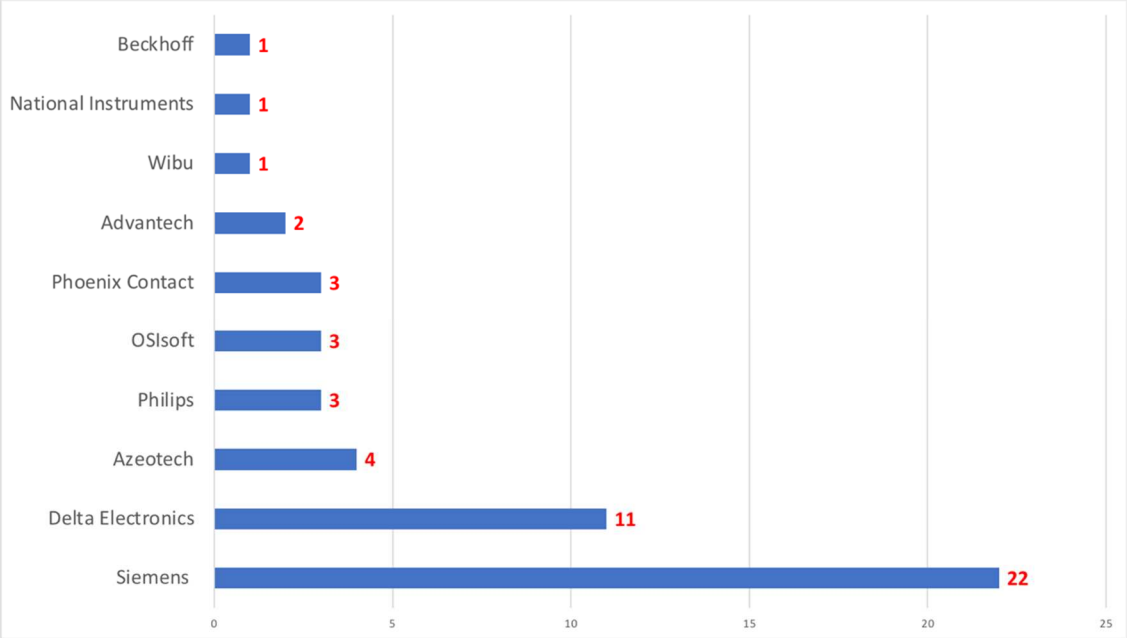
In the case of **Azeotech**, the **4** published **weaknesses** are associated with its Daqfactory product and affect all versions up to 1.8.1. The ICS-CERT / CISA has issued an alert on these weaknesses (**ICSA-21-308-02**), although their CVSS V2 evaluations do not qualify them as CCI thermometer alerts as their complexity is Medium or high.

The popular manufacturer **OSIsoft** sees **3** published **weaknesses** that affect its PIVision and PIServer products. The ICS-CERT / CISA has published 2 related alerts (**ICSA-21-313-05 and ICSA-21-313-06**), although according to the criteria of the CCI thermometer on alerts, they are not classified as such.

New weaknesses

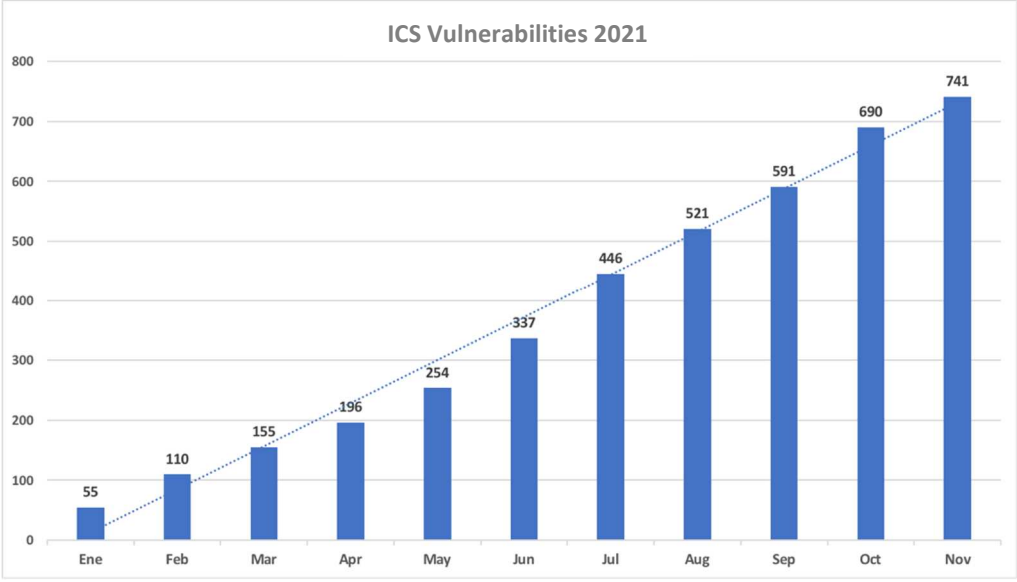
The number of ICS vulnerabilities published and **fully characterized** by NIST since the last update is **51**.

Once again, Siemens stands out among the manufacturers studied:



The detail of these weaknesses characterized in November can be found in **ANNEX II**.

At the end of 2021, we can see that the trend in the investigation of weaknesses in the control systems used in multiple sectors continues to grow steadily.

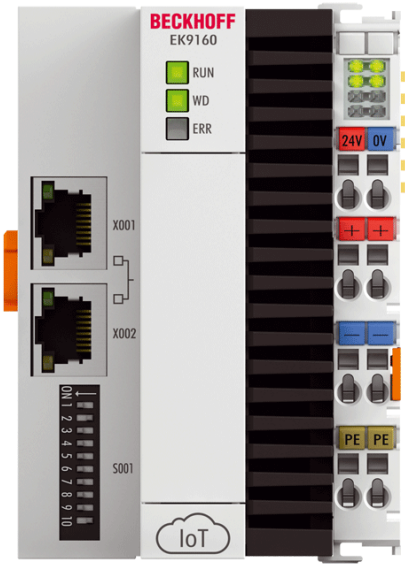


New alerts

This month, NIST has released (fully characterized) 1 new manufacturer alert.

We recall that they are classified as alerts given that the exploitation of the vulnerability has a low complexity, has the network as an access vector and can cause a total loss of service. (Based on CVSS V2 classification, to allow historical classification of weaknesses in older products).

Beckhoff has seen 1 alert posted about its TwinCAT OPC UA Server TF6100 and TS6100 products:



Beckhoff EK9160

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-34594	2021-11-04	8.5	⚠	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system.

Considering the implementation that the OPC UA protocol has in IoT solutions, we must review the potential impact of this weakness in industrial digitization projects in implementation or in those recently implemented.

Risk map

November 30, 2021

	Circutor	Dahua		
Digitek Hikvision Johnson Controls Motorola Solutions Pro-face Zebra Industrial	Advantech Auvesy B. Braun Medical Beckhoff Bosch Emerson Delta Electronics Hilscher Miitsubishi Electric Morpho Moxa Panasonic Phoenix Contact RugggedCom Schneider Electric Wago			Siemens
ABB Belden CODESYS Digi Eaton eWON Fatek Fuji Electric Hirschmann Honeywell Kepware LAquis SCADA Omron PTC (ThingWorx) QNX Rockwell Software Toolbox Wibu Systems Wind River	GE Mikrotik			
Aveva Azeotech National Instruments OSIsoft Philips ProSoft SafeNet SearchBlox Tesla Trane				

Changes in manufacturing risk

Beckhoff increases his exposure on the Risk Map with a Medium + value, due to the publication of 1 alert in November. This manufacturer has seen 18 CVEs published in 2021 and its average CVSS V2 of the last 10 years is 5.4.

OSIsoft and Azeotech enter the risk map directly with a Low risk

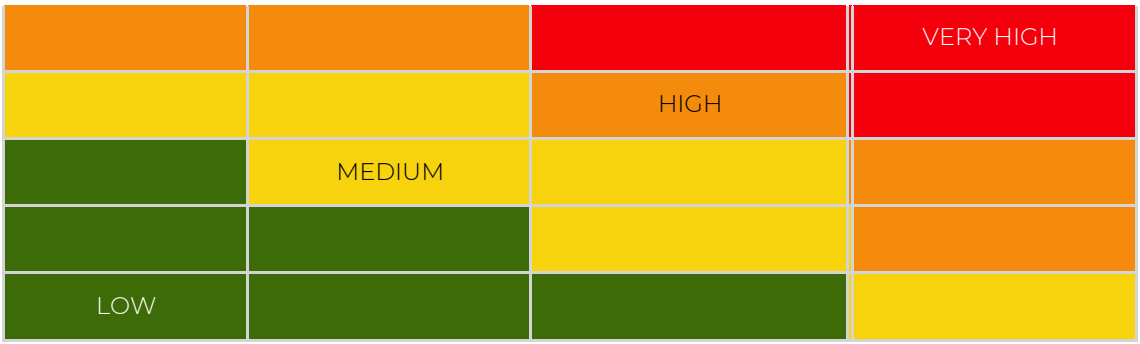
In the case of Azeotech, the 4 published weaknesses are associated with its Daqfactory product and affect all versions up to 1.8.1. The average CVSS V2 value of this manufacturer in the last 10 years becomes 5.8.

The popular manufacturer OSIsoft sees 3 published weaknesses that affect its PIVision and PIServer products. This establishes an average CVSS V2 value for this manufacturer of 4.7 over the last 10 years.

The rest of the manufacturers maintain their level in the qualitative heat map of risk exposure and highlight the 241 vulnerabilities published by the NIST in 2021 for the manufacturer Siemens.

ANNEX – I: Risk map calculation

In order to show the position of each manufacturer graphically and quickly in relation to the risk associated with the published vulnerabilities, I have selected a very common graphic format in Risk management: the heat map.
This diagram presents different colours to represent the associated risk in a qualitative way and in four ranges: Low, Medium, High and Very High.



The position of each manufacturer within the map depends on the values obtained in two parameters associated with the **probability** (Number of CVEs published) and the **impact** of those CVEs (CVSS average value).
For each year, each of these values has been calculated between 1 and 5.

- On the horizontal axis, the value proportional to the number of CVEs published for that manufacturer in a specific year has been calculated compared to the manufacturer with the highest number of CVEs.
- On the vertical axis, the average CVSS value of the CVEs published that year was calculated and divided by 2.

To try to give a more qualitative idea regarding the position of each manufacturer, two corrections have been introduced in the calculation:

- In the manufacturer has any CVE that year considered as **Alert** (Access by network, low complexity, and full impact on availability), the impact is increased by one unit (vertical axis) and by one unit the probability (horizontal axis). This is done to differentiate this manufacturer from others without this type of CVEs and position it in a higher risk area.
- In the same way, if a manufacturer has a CVE that year with a CVSS value of 10.0, the probability (horizontal axis) is increased by one unit. This is done to differentiate this manufacturer from others without this type of CVEs and position it in a higher risk area.

It has been studied through different simulations that these corrections do not suppose great alterations in the global risk posture of that manufacturer and, nevertheless, they present a more adjusted qualitative diagnosis.

ANNEX II – Vulnerabilities published by NIST since the last CCI Thermometer

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-34594	2021-11-04	8.5	⚠	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system.
CVE-2021-26262	2021-11-19	5.0		Philips MRI 1.5T and MRI 3T Version 5.x.x does not restrict or incorrectly restricts access to a resource from an unauthorized actor.
CVE-2021-26248	2021-11-19	2.1		Philips MRI 1.5T and MRI 3T Version 5.x.x assigns an owner who is outside the intended control sphere to a resource.
CVE-2021-42744	2021-11-19	2.1		Philips MRI 1.5T and MRI 3T Version 5.x.x exposes sensitive information to an actor not explicitly authorized to have access.
CVE-2021-43549	2021-11-18	3.5		A remote authenticated attacker with write access to a PI Server could trick a user into interacting with a PI Web API endpoint and redirect them to a malicious website. As a result, a victim may disclose sensitive information to the attacker or be provided with false information.
CVE-2021-43553	2021-11-17	4.0		PI Vision could disclose information to a user with insufficient privileges for an AF attribute that is the child of another attribute and is configured as a Limits property.
CVE-2021-43551	2021-11-17	3.5		A remote attacker with write access to PI Vision could inject code into a display. Unauthorized information disclosure, modification, or deletion is possible if a victim views or interacts with the infected display using Microsoft Internet Explorer. The impact affects PI System data and other data accessible with victim's user permissions.
CVE-2021-42706	2021-11-15	4.6		This vulnerability could allow an attacker to disclose information and execute arbitrary code on affected installations of WebAccess/MHI Designer
CVE-2021-42703	2021-11-15	4.3		This vulnerability could allow an attacker to send malicious Javascript code resulting in hijacking of the user's cookie/session tokens, redirecting the user to a malicious webpage, and performing unintended browser action.
CVE-2021-41057	2021-11-14	3.6		In WIBU CodeMeter Runtime before 7.30a, creating a crafted CmDongles symbolic link will overwrite the linked file without checking permissions.
CVE-2021-42563	2021-11-12	4.6		There is an Unquoted Service Path in NI Service Locator (nisvcloc.exe) in versions prior to 18.0 on Windows. This may allow an authorized local user to insert arbitrary code into the unquoted service path and escalate privileges.
CVE-2021-34598	2021-11-10	4.3		In Phoenix Contact FL MGUARD 1102 and 1105 in Versions 1.4.0, 1.4.1 and 1.5.0 the remote logging functionality is impaired by the lack of memory release for data structures from syslog-ng when remote logging is active
CVE-2021-34582	2021-11-10	3.5		In Phoenix Contact FL MGUARD 1102 and 1105 in Versions 1.4.0, 1.4.1 and 1.5.0 a user with high privileges can inject HTML code (XSS) through web-based management or the REST API with a manipulated certificate file.
CVE-2021-40358	2021-11-09	7.5		A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). Legitimate file operations of the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read, write or delete unexpected critical files.
CVE-2021-31884	2021-11-09	7.5		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application assumes that the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014)
CVE-2021-31886	2021-11-09	7.5		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions),

CVE	Date published	CVSS V2	Warning	Description
				APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010)
CVE-2021-37207	2021-11-09	7.2		A vulnerability has been identified in SENTRON powermanager V3 (All versions). The affected application assigns improper access rights to a specific folder containing configuration files. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.
CVE-2021-31887	2021-11-09	6.5		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016)
CVE-2021-31888	2021-11-09	6.5		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018)
CVE-2021-31345	2021-11-09	6.4		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006)
CVE-2021-31889	2021-11-09	6.4		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015)
CVE-2021-31890	2021-11-09	6.4		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017)
CVE-2021-31346	2021-11-09	6.4		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC

CVE	Date published	CVSS V2	Warning	Description
				Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007)
CVE-2021-40366	2021-11-09	5.8		A vulnerability has been identified in Climatix POL909 (AWM module) (All versions < V11.34). The web server of affected devices transmits data without TLS encryption. This could allow an unauthenticated remote attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit.
CVE-2021-42021	2021-11-09	5.0		A vulnerability has been identified in Siveillance Video DLNA Server (2019 R1), Siveillance Video DLNA Server (2019 R2), Siveillance Video DLNA Server (2019 R3), Siveillance Video DLNA Server (2020 R1), Siveillance Video DLNA Server (2020 R2), Siveillance Video DLNA Server (2020 R3), Siveillance Video DLNA Server (2021 R1). The affected application contains a path traversal vulnerability that could allow to read arbitrary files on the server that are outside the application's web document directory. An unauthenticated remote attacker could exploit this issue to access sensitive information for subsequent attacks.
CVE-2021-40359	2021-11-09	5.0		A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). When downloading files, the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read unexpected critical files.
CVE-2021-40364	2021-11-09	5.0		A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC V15 and earlier (All versions), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V7.4 and earlier (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). The affected systems store sensitive information in log files. An attacker with access to the log files could publicly expose the information or reuse it to develop further attacks on the system.
CVE-2021-31881	2021-11-09	5.0		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008)
CVE-2021-31883	2021-11-09	5.0		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013)
CVE-2021-31882	2021-11-09	5.0		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011)
CVE-2021-31885	2021-11-09	5.0		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009)

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-31344	2021-11-09	5.0		A vulnerability has been identified in APOGEE MBC (PPC) (BACnet) (All versions), APOGEE MBC (PPC) (P2 Ethernet) (All versions), APOGEE MEC (PPC) (BACnet) (All versions), APOGEE MEC (PPC) (P2 Ethernet) (All versions), APOGEE PXC Compact (BACnet) (All versions), APOGEE PXC Compact (P2 Ethernet) (All versions), APOGEE PXC Modular (BACnet) (All versions), APOGEE PXC Modular (P2 Ethernet) (All versions), Capital VSTAR (All versions), Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions < V2017.02.4), Nucleus ReadyStart V4 (All versions < V4.1.1), Nucleus Source Code (All versions), TALON TC Compact (BACnet) (All versions), TALON TC Modular (BACnet) (All versions). ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004)
CVE-2020-10052	2021-11-09	2.1		A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.12). The affected application writes sensitive data, such as usernames and passwords in log files. A local attacker with access to the log files could use this information to launch further attacks.
CVE-2020-10053	2021-11-09	2.1		A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.12). The affected application writes sensitive data, such as database credentials in configuration files. A local attacker with access to the configuration files could use this information to launch further attacks.
CVE-2020-10054	2021-11-09	2.1		A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V2.12). The affected application does not properly handle the import of large configuration files. A local attacker could import a specially crafted file which could lead to a denial-of-service condition of the application service.
CVE-2021-42543	2021-11-05	7.5		The affected application uses specific functions that could be abused through a crafted project file, which could lead to code execution, system reboot, and system shutdown.
CVE-2021-42698	2021-11-05	6.8		Project files are stored memory objects in the form of binary serialized data that can later be read and deserialized again to instantiate the original objects in memory. Malicious manipulation of these files may allow an attacker to corrupt memory.
CVE-2021-42699	2021-11-05	4.3		The affected product is vulnerable to cookie information being transmitted as cleartext over HTTP. An attacker can capture network traffic, obtain the user's cookie and take over the account.
CVE-2021-42701	2021-11-05	2.6		An attacker could prepare a specially crafted project file that, if opened, would attempt to connect to the cloud and trigger a man in the middle (MiTM) attack. This could allow an attacker to obtain credentials and take over the user's cloud account.
CVE-2021-34597	2021-11-04	6.8		Improper Input Validation vulnerability in PC Worx Automation Suite of Phoenix Contact up to version 1.88 could allow an attacker with a manipulated project file to unpack arbitrary files outside of the selected project directory.
CVE-2021-38424	2021-11-03	6.8		The tag interface of Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to an attacker injecting formulas into the tag data. Those formulas may then be executed when it is opened with a spreadsheet application.
CVE-2021-38422	2021-11-03	4.6		Delta Electronics DIALink versions 1.2.4.0 and prior stores sensitive information in cleartext, which may allow an attacker to have extensive access to the application directory and escalate privileges.
CVE-2021-38420	2021-11-03	4.6		Delta Electronics DIALink versions 1.2.4.0 and prior default permissions give extensive permissions to low-privileged user accounts, which may allow an attacker to modify the installation directory and upload malicious files.
CVE-2021-38416	2021-11-03	4.4		Delta Electronics DIALink versions 1.2.4.0 and prior insecurely loads libraries, which may allow an attacker to use DLL hijacking and takeover the system where the software is installed.
CVE-2021-38418	2021-11-03	4.3		Delta Electronics DIALink versions 1.2.4.0 and prior runs by default on HTTP, which may allow an attacker to be positioned between the traffic and perform a machine-in-the-middle attack to access information without authorization.
CVE-2021-38403	2021-11-03	3.5		Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter supplier of the API maintenance, which may allow an attacker to remotely execute code.
CVE-2021-38428	2021-11-03	3.5		Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter name of the API schedule, which may allow an attacker to remotely execute code.
CVE-2021-38407	2021-11-03	3.5		Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter name of the API devices, which may allow an attacker to remotely execute code.
CVE-2021-38411	2021-11-03	3.5		Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter deviceName of the API modbusWriter-Reader, which may allow an attacker to remotely execute code.
CVE-2021-38488	2021-11-03	3.5		Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter comment of the API events, which may allow an attacker to remotely execute code.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-22278	2021-10-28	4.6		A certificate validation vulnerability in PCM600 Update Manager allows attacker to get unwanted software packages to be installed on computer which has PCM600 installed.