Industrial Cybersecurity Center

ICS Vulnerabilities
CCI Thermometer
2021- 6

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

Introduction **4**
2021 Developments 4
Manufacturers and ICS weaknesses **5**
New manufacturers 5
New weaknesses 6
New alerts 7
Risk map **9**
Changes in manufacturing risk 10
ANNEX – I: Risk map calculation **10**
ANNEX II – Vulnerabilities published by NIST since the last CCI Thermometer **12**

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 CCI 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**.

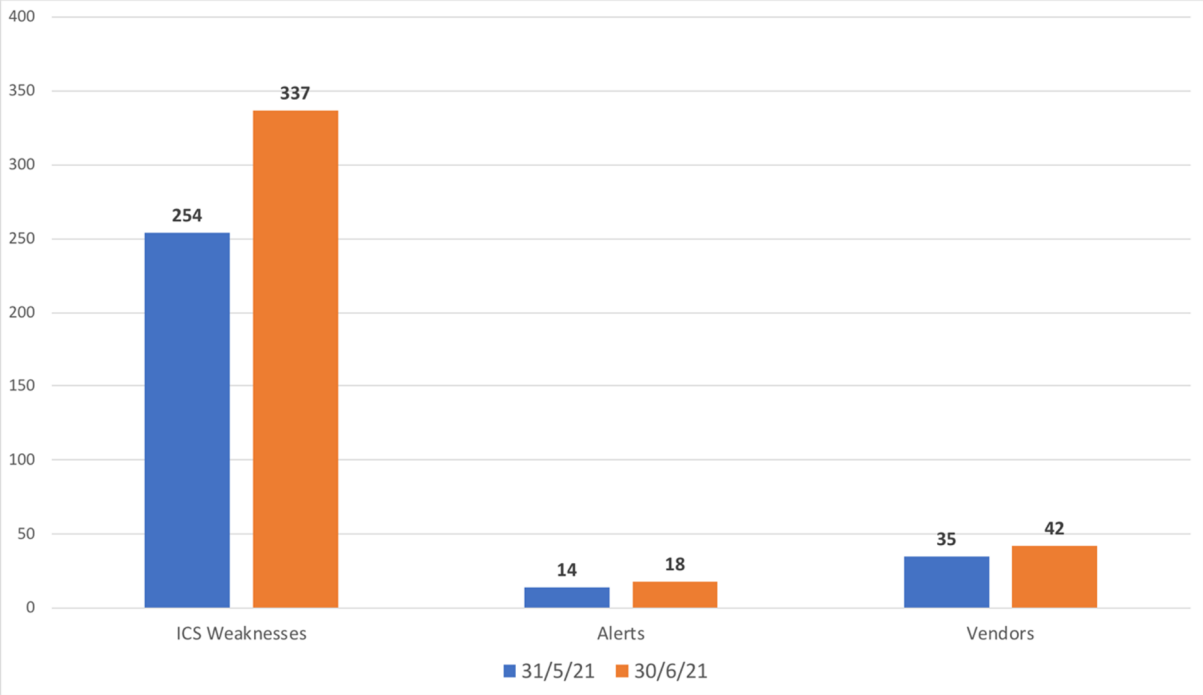
In each update we will publish:

- **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, 7 new **manufacturers** are included, and their number increases to **42**:

Low Risk	Medium Risk	High Risk	Very High Risk
Aveva CODESYS Johnson Controls SafeNet Wibu	Digitek	Circutor	N/A

In this edition, the list of control system manufacturers has been updated with two Spanish companies that deploy their products in critical infrastructures in different sectors: **Digitek** and **Circutor**. I think this is necessary since they are not on the list of manufacturers of the ICS-CERT Advisories, they can be installed in Spanish and foreign operators, and their contribution to the quantitative risk analysis is marginal due to their number.

- The vulnerability CVE-2021-3604, discovered by **Ander Martínez** from TITANIUM Industrial Security, affects the Evalos8 product (**Primion-Digitek**), specifically in version v1.0.1.55 of the Secure8 module. Primion-Digitek specializes in the implementation of access controls, signing, personnel control, etc. They have their systems implemented in critical infrastructures, such as airports, electrical industries, hospitals, as well as in public administration buildings, and it is a clear example that physical and logical security (IT and OT) must be addressed in a uniform manner. in organizations that provide essential services.

- • The vulnerabilities CVE-2021-33841 and CVE-2021-33842 have been managed by our CCI colleague **Aarón Flecha** and affect the firmware of the product Circutor SGE-PLC1000, the first one being an alert since it allows a remote user, in a relatively simple way, it can cause the unavailability of the device and its services, and even cause other damages to other devices in the same network given its role in it. Because of this, Circutor enters the risk exposure map directly with a High Value.

In the case of **Wibu Systems**, two new vulnerabilities (CVE-2021-20093 and CVE-2021-20094) have been published on its CodeMeter product. As we discussed last year, it is a clear example of **amplified vulnerabilities** that can affect third-party products such as ABB, Bosch, Phoenix Contact, Schneider Electric, Siemens, etc.

CODESYS is another case of vulnerability amplification, since its PLC programming solutions are used by Beckhoff, Kontron, Moeller, Festo and Mitsubishi among others.

Aveva has seen another vulnerability published in its product InTouch Runtime 2020 R2, although with a relatively low impact. (CVSS 2.1)

New weaknesses

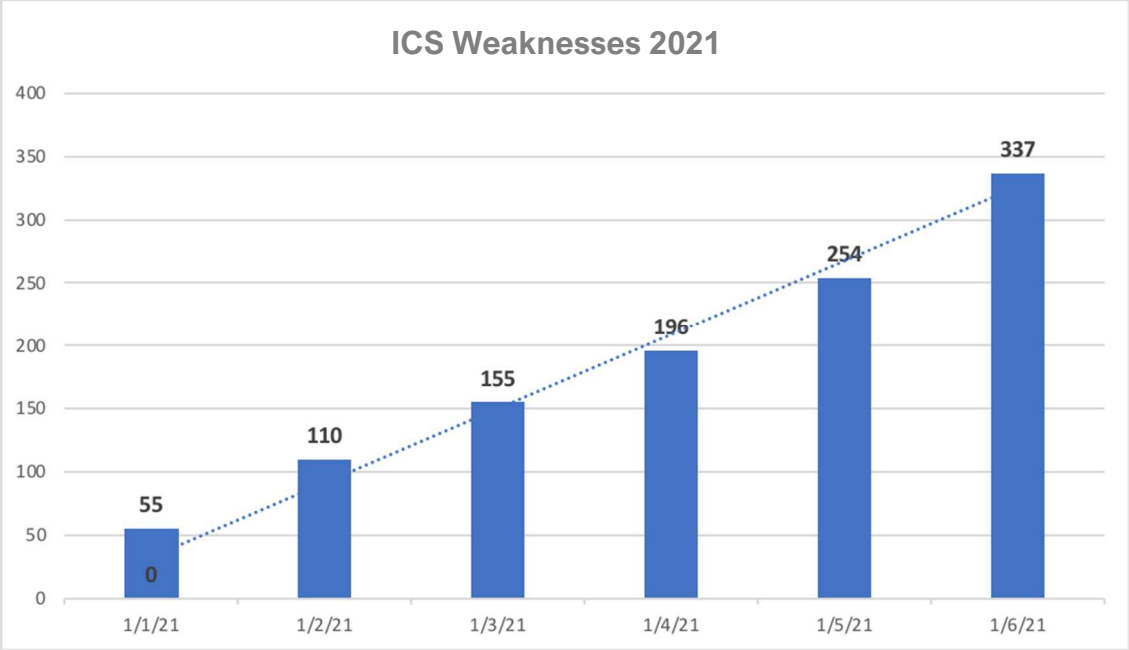
The number of ICS vulnerabilities released by NIST since the last update is **83**.

Two manufacturers accumulate almost 50% of this number:

- **Schneider Electric**, with **23** weaknesses published in June 2021 associated with its products, is the manufacturer that registers the most weaknesses. Additionally, the publication of **2 alerts** about any of these weaknesses has worsened its exposure to risk, as we will see in the next point.
- **CODESYS** with **15** weaknesses on its products, and which are also used by third-party manufacturers.
- **Siemens** with **8** CVEs published in June continues to lead the qualitative risk map. It is noteworthy that to this date, more vulnerabilities have been published on its products (**102**) than in the entire year 2020 (**95**).

The cases of **CODESYS** and **Wibu**, make us comment again on the amplification of vulnerabilities due to the use of libraries and third-party solutions, mainly due to the saving of time in the launch of new products, and to the multiple acquisitions of products by of the big control systems companies. **The development and implementation of maintenance tools for the Software Bill of Materials (SBOM) and the control of the supply chain in the secure development of applications should be promoted in the near future to mitigate these risks to production.**

At the equator 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 **4 new manufacturer alerts**. We recall that they are classified as alerts given that the exploitation of the vulnerability has 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).

The first of these alerts is associated with an uncontrolled resource consumption problem in **Mitsubishi Electric** MELSEC iQ-R series CPU modules (R00 / 01 / 02CPU all versions, R04 / 08/16/32/120 (EN) CPU all versions, R08 / 16/32 / 120SFCPU all versions, R08 / 16/32 / 120PCPU all versions, R08 / 16/32 / 120PSFCPU all versions), which allows an unauthenticated remote attacker to prevent Legitimate clients connect to the MELSOFT transmission port (TCP / IP) by failing to close a connection properly, which can lead to a **denial of service** (DoS) condition.

Mitsubishi Electric MELSEC iQ-R series

CVE	Date published	CVSS	Warning	Description
CVE-2021-20591	2021-06-11	7.8	⚠	Uncontrolled Resource Consumption vulnerability in Mitsubishi Electric MELSEC iQ-R series CPU modules (R00/01/02CPU all versions, R04/08/16/32/120(EN)CPU all versions, R08/16/32/120SFCPU all versions, R08/16/32/120PCPU all versions, R08/16/32/120PSFCPU all versions) allows a remote unauthenticated attacker to prevent legitimate clients from connecting to the MELSOFT transmission port (TCP/IP) by not closing a connection properly, which may lead to a denial of service (DoS) condition.

Schneider Electric has seen **2 alerts** posted about 2 of its product series:

Modicon M241/M251

PowerLogic PM55xx

CVE	Date published	CVSS	Warning	Description
CVE-2021-22763	2021-06-11	10.0	⚠	A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists in PowerLogic PM55xx, PowerLogic PM8ECC, PowerLogic EGX100 and PowerLogic EGX300 (see security notification for version infromation) that could allow an attacker administrator level access to a device.
CVE-2021-22699	2021-06-11	7.8	⚠	Improper Input Validation vulnerability exists in Modicon M241/M251 logic controllers firmware prior to V5.1.9.1 that could cause denial of service when specific crafted requests are sent to the controller over HTTP.

Circutor has seen **an alert** published by NIST about one of its products:

Circutor SGE-PLC1000

The SGE-PLC1000 unit is a communications concentrator in charge of managing and reading three-phase and single-phase energy meters with PRIME communications connected to the same low voltage network.

This vulnerability would allow an attacker with access to the network where the vulnerable device is located would be able to send tailor-made requests to take control of the device itself and make changes at will.

CVE	Date published	CVSS	Warning	Description
CVE-2021-33841	2021-06-09	10.0	⚠	SGE-PLC1000 device, in its 0.9.2b firmware version, does not handle some requests correctly, allowing a remote attacker to inject code into the operating system with maximum privileges.

Risk map

June 30, 2021

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

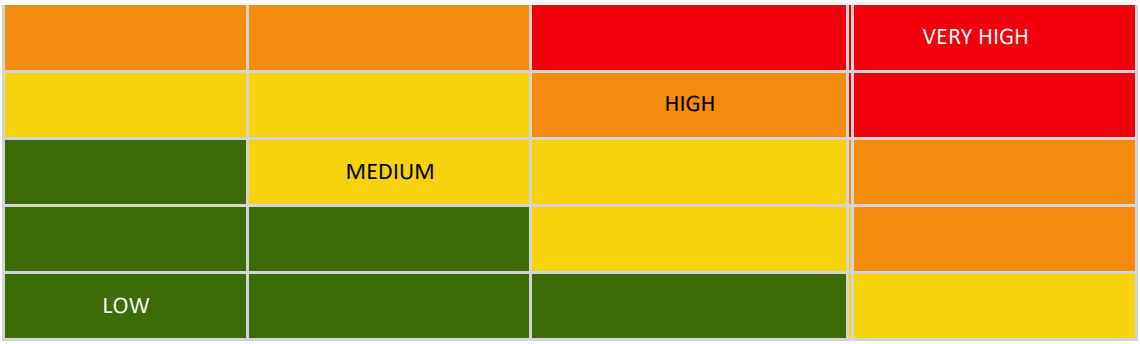
Changes in manufacturing risk

Due to the high number of weaknesses published by NIST in June on Schneider Electric products, and the existence of alerts, it has put its risk exposure to the edge of High (Medium ++) risk.

Paradoxically, **CODESYS** and **Wibu**, despite potentially impacting a large number of products from other manufacturers, remain in the low risk zone, since their products obtain an average CVSS V2 of **6.8** and **5.5** respectively in the last 10 years.

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-2021-3604	2021-06-18	7.5		Secure 8 (Evalos) does not validate user input data correctly, allowing a remote attacker to perform a Blind SQL Injection. An attacker could exploit this vulnerability in order to extract information of users and administrator accounts stored in the database.
CVE-2021-20591	2021-06-11	7.8	⚠	Uncontrolled Resource Consumption vulnerability in Mitsubishi Electric MELSEC iQ-R series CPU modules (R00/01/02CPU all versions, R04/08/16/32/120(EN)CPU all versions, R08/16/32/120SFCPU all versions, R08/16/32/120PCPU all versions, R08/16/32/120PSFCPU all versions) allows a remote unauthenticated attacker to prevent legitimate clients from connecting to the MELSOFT transmission port (TCP/IP) by not closing a connection properly, which may lead to a denial of service (DoS) condition.
CVE-2021-22763	2021-06-11	10.0	⚠	A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists in PowerLogic PM55xx, PowerLogic PM8ECC, PowerLogic EGX100 and PowerLogic EGX300 (see security notification for version infromation) that could allow an attacker administrator level access to a device.
CVE-2021-22699	2021-05-26	7.8	⚠	Improper Input Validation vulnerability exists in Modicon M241/M251 logic controllers firmware prior to V5.1.9.1 that could cause denial of service when specific crafted requests are sent to the controller over HTTP.
CVE-2021-32954	2021-06-18	6.8		Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to a directory traversal, which may allow an attacker to remotely read arbitrary files on the file system.
CVE-2021-32956	2021-06-18	5.8		Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to redirection, which may allow an attacker to send a maliciously crafted URL that could result in redirecting a user to a malicious webpage.
CVE-2021-33824	2021-06-18	5.0		An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service.
CVE-2021-33823	2021-06-18	5.0		An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service.
CVE-2021-31477	2021-06-16	7.5		This vulnerability allows remote attackers to execute arbitrary code on affected installations of GE Reason RPV311 14A03. Authentication is not required to exploit this vulnerability. The specific flaw exists within the firmware and filesystem of the device. The firmware and filesystem contain hard-coded default credentials. An attacker can leverage this vulnerability to execute code in the context of the download user. Was ZDI-CAN-11852.
CVE-2021-20093	2021-06-16	6.4		A buffer over-read vulnerability exists in Wibu-Systems CodeMeter versions < 7.21a. An unauthenticated remote attacker can exploit this issue to disclose heap memory contents or crash the CodeMeter Runtime Server.
CVE-2021-20094	2021-06-16	5.0		A denial of service vulnerability exists in Wibu-Systems CodeMeter versions < 7.21a. An unauthenticated remote attacker can exploit this issue to crash the CodeMeter Runtime Server.
CVE-2021-28979	2021-06-16	4.3		SafeNet KeySecure Management Console 8.12.0 is vulnerable to HTTP response splitting attacks. A remote attacker could exploit this vulnerability using specially-crafted URL to cause the server to return a split response, once the URL is clicked.
CVE-2021-27388	2021-06-15	7.5		SINAMICS medium voltage routable products are affected by a vulnerability in the Sm@rtServer component for remote access that could allow an unauthenticated attacker to cause a denial-of-service condition, and/or execution of limited configuration modifications and/or execution of limited control commands on the SINAMICS Medium Voltage Products, Remote Access (SINAMICS SL150: All versions, SINAMICS SM150: All versions, SINAMICS SM150i: All versions).
CVE-2021-26845	2021-06-14	5.0		Information Exposure vulnerability in Hitachi ABB Power Grids eSOMS allows unauthorized user to gain access to report data if the URL used to access the report is discovered. This issue affects: Hitachi ABB Power Grids eSOMS 6.0 versions prior to 6.0.4.2.2; 6.1 versions prior to 6.1.4; 6.3 versions prior to 6.3.
CVE-2021-27887	2021-06-14	3.5		Cross-site Scripting (XSS) vulnerability in the main dashboard of Ellipse APM versions allows an authenticated user or integrated application to inject malicious data into the application that can then be executed in a victim's browser. This issue affects: Hitachi ABB Power Grids Ellipse APM 5.3 version 5.3.0.1 and prior versions; 5.2 version 5.2.0.3 and prior versions; 5.1 version 5.1.0.6 and prior versions.
CVE-2021-32930	2021-06-11	7.5		The affected product's configuration is vulnerable due to missing authentication, which may allow an attacker to change configurations and execute arbitrary code on the iView (versions prior to v5.7.03.6182).

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-22758	2021-06-11	6.8		A CWE-824: Access of uninitialized pointer vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to lack validation of user-supplied input data, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22752	2021-06-11	6.8		A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing size checks, when a malicious WSP (Workspace) file is being parsed by IGSS Definition.
CVE-2021-22754	2021-06-11	6.8		A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to lack of proper validation of user-supplied data, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22755	2021-06-11	6.8		A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied data, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22751	2021-06-11	6.8		A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or execution of arbitrary code due to lack of input validation, when a malicious CGF (Configuration Group File) file is imported to IGSS Definition.
CVE-2021-22750	2021-06-11	6.8		A CWE-787: Out-of-bounds write vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21041 and prior that could result in loss of data or remote code execution due to missing length checks, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22760	2021-06-11	6.8		A CWE-763: Release of invalid pointer or reference vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing checks of user-supplied input data, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22759	2021-06-11	6.8		A CWE-416: Use after free vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to use of unchecked input data, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22762	2021-06-11	6.8		A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in remote code execution, when a malicious CGF or WSP file is being parsed by IGSS Definition.
CVE-2021-22753	2021-06-11	6.8		A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in loss of data or remote code execution due to missing length checks, when a malicious WSP file is being parsed by IGSS Definition.
CVE-2021-22756	2021-06-11	6.8		A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of user-supplied data validation, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22757	2021-06-11	6.8		A CWE-125: Out-of-bounds read vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied input data, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22761	2021-06-11	6.8		A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists inIGSS Definition (Def.exe) V15.0.0.21140 and prior that could result in disclosure of information or remote code e+F15xecution due to missing length check on user supplied data, when a malicious CGF file is imported to IGSS Definition.
CVE-2021-22764	2021-06-11	5.0		A CWE-287: Improper Authentication vulnerability exists in PowerLogic PM55xx, PowerLogic PM8ECC, PowerLogic EGX100 and PowerLogic EGX300 (see security notification for version infromation) that could cause loss of connectivity to the device via Modbus TCP protocol when an attacker sends a specially crafted HTTP request.
CVE-2021-22749	2021-06-11	5.0		A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists in Modicon X80 BMXNOR0200H RTU SV1.70 IR22 and prior that could cause information leak concerning the current RTU configuration including communication parameters dedicated to telemetry, when a specially crafted HTTP request is sent to the web server of the module.
CVE-2021-32932	2021-06-11	5.0		The affected product is vulnerable to a SQL injection, which may allow an unauthorized attacker to disclose information on the iView (versions prior to v5.7.03.6182).
CVE-2021-34540	2021-06-11	4.3		Advantech WebAccess 8.4.2 and 8.4.4 allows XSS via the username column of the bwRoot.asp page of WADashboard.
CVE-2021-22769	2021-06-11	4.0		A CWE-269: Improper Privilege Management vulnerability exists in EnerlinÕX ComÕX versions prior to V6.8.4 that could cause disclosure of device configuration information to any authenticated user when a specially crafted request is sent to the device.
CVE-2021-32942	2021-06-09	2.1		The vulnerability could expose cleartext credentials from AVEVA InTouch Runtime 2020 R2 and all prior versions (WindowViewer) if an authorized, privileged user creates a diagnostic memory dump of the process and saves it to a non-protected location.
CVE-2021-33841	2021-06-09	10.0		SGE-PLC1000 device, in its 0.9.2b firmware version, does not handle some requests correctly, allowing a remote attacker to inject code into the operating system with maximum privileges.
CVE-2021-33842	2021-06-09	7.7		Improper Authentication vulnerability in the cookie parameter of Circutor SGE-PLC1000 firmware version 0.9.2b allows an attacker to perform operations as an authenticated user. In order to exploit this vulnerability, the attacker must be within the network where the device affected is located.
CVE-2021-31342	2021-06-08	6.8		The ugeom2d.dll library in all versions of Solid Edge SE2020 before 2020MP14 and all versions of Solid Edge SE2021 before SE2021MP5 lack proper validation of user-supplied data when parsing DFT files. This could result in an out-of-bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-31343	2021-06-08	6.8		The jutil.dll library in all versions of Solid Edge SE2020 before 2020MP14 and all versions of Solid Edge SE2021 before SE2021MP5 lack proper validation of user-supplied data when parsing DFT files. This could result in an out-of-bounds write past the end of an allocation structure. An attacker could leverage this vulnerability to execute code in the context of the current process.
CVE-2021-27387	2021-06-08	6.8		A vulnerability has been identified in Simcenter Femap 2020.2 (All versions < V2020.2.MP3), Simcenter Femap 2021.1 (All versions < V2021.1.MP3). The femap.exe application lacks proper validation of user-supplied data when parsing FEMAP files. This could result in an out of bounds write past the end of an allocated structure, a different vulnerability than CVE-2021-27399. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12819)
CVE-2021-27399	2021-06-08	6.8		A vulnerability has been identified in Simcenter Femap 2020.2 (All versions < V2020.2.MP3), Simcenter Femap 2021.1 (All versions < V2021.1.MP3). The femap.exe application lacks proper validation of user-supplied data when parsing FEMAP files. This could result in an out of bounds write past the end of an allocated structure, a different vulnerability than CVE-2021-27387. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12820)
CVE-2021-27390	2021-06-08	6.8		A vulnerability has been identified in JT2Go (All versions < V13.1.0.3), Teamcenter Visualization (All versions < V13.1.0.3). The TIFF_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13131)
CVE-2021-31340	2021-06-08	5.0		A vulnerability has been identified in SIMATIC RF166C (All versions > V1.1 and < V1.3.2), SIMATIC RF185C (All versions > V1.1 and < V1.3.2), SIMATIC RF186C (All versions > V1.1 and < V1.3.2), SIMATIC RF186CI (All versions > V1.1 and < V1.3.2), SIMATIC RF188C (All versions > V1.1 and < V1.3.2), SIMATIC RF188CI (All versions > V1.1 and < V1.3.2), SIMATIC RF360R (All versions), SIMATIC RF615R (All versions > V3.0), SIMATIC RF680R (All versions > V3.0), SIMATIC RF685R (All versions > V3.0). Affected devices do not properly handle large numbers of incoming connections. An attacker may leverage this to cause a Denial-of-Service situation.
CVE-2021-27657	2021-06-04	6.5		Successful exploitation of this vulnerability could give an authenticated Metasys user an unintended level of access to the server file system, allowing them to access or modify system files by sending specifically crafted web messages to the Metasys system. This issue affects: Johnson Controls Metasys version 11.0 and prior versions.
CVE-2021-32926	2021-06-03	5.0		When an authenticated password change request takes place, this vulnerability could allow the attacker to intercept the message that includes the legitimate, new password hash and replace it with an illegitimate hash. The user would no longer be able to authenticate to the controller (Micro800: All versions, MicroLogix 1400: Version 21 and later) causing a denial-of-service condition
CVE-2020-15782	2021-05-28	7.5		A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected devices are vulnerable to a memory protection bypass through a specific operation. A remote unauthenticated attacker with network access to port 102/tcp could potentially write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks.
CVE-2021-22735	2021-05-26	6.5		Improper Verification of Cryptographic Signature vulnerability exists inhomeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could allow remote code execution when unauthorized code is copied to the device.
CVE-2021-22734	2021-05-26	6.5		Improper Verification of Cryptographic Signature vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause remote code execution when an attacker loads unauthorized code.
CVE-2021-22738	2021-05-26	5.0		Use of a Broken or Risky Cryptographic Algorithm vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior that could cause unauthorized access when credentials are discovered after a brute force attack.
CVE-2021-22737	2021-05-26	5.0		Insufficiently Protected Credentials vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior that could cause unauthorized access of when credentials are discovered after a brute force attack.
CVE-2021-22736	2021-05-26	5.0		Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause a denial of service when an unauthorized file is uploaded.
CVE-2021-22733	2021-05-26	4.6		Improper Privilege Management vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause shell access when unauthorized code is loaded into the system folder.
CVE-2021-22732	2021-05-26	4.6		Improper Privilege Management vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause a code execution issue when an attacker loads unauthorized code on the web server.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-22705	2021-05-26	4.6		Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause denial of service or unauthorized access to system information when interacting directly with a driver installed by Vijeo Designer or EcoStruxure Machine Expert
CVE-2021-22741	2021-05-26	4.6		Use of Password Hash with Insufficient Computational Effort vulnerability exists in ClearSCADA (all versions), EcoStruxure Geo SCADA Expert 2019 (all versions), and EcoStruxure Geo SCADA Expert 2020 (V83.7742.1 and prior), which could cause the revealing of account credentials when server database files are available. Exposure of these files to an attacker can make the system vulnerable to password decryption attacks. Note that ".sde" configuration export files do not contain user account password hashes.
CVE-2021-22739	2021-05-26	4.3		Information Exposure vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause a device to be compromised when it is first configured.
CVE-2021-22740	2021-05-26	4.0		Information Exposure vulnerability exists in homeLYnk (Wiser For KNX) and spaceLYnk V2.60 and prior which could cause information to be exposed when an unauthorized file is uploaded.
CVE-2021-22743	2021-05-26	2.1		Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex TCM 4351B installed on Tricon V11.3.x systems that could cause module reset when TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position.
CVE-2021-22742	2021-05-26	2.1		Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module reset when TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position.
CVE-2021-22744	2021-05-26	2.1		Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module reset when TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22745, CVE-2021-22746, and CVE-2021-22747.
CVE-2021-22745	2021-05-26	2.1		Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module reset when TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22744, CVE-2021-22746, and CVE-2021-22747.
CVE-2021-22746	2021-05-26	2.1		Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module reset when TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22744, CVE-2021-22745, and CVE-2021-22747.
CVE-2021-22747	2021-05-26	2.1		Improper Check for Unusual or Exceptional Conditions vulnerability exists in Triconex Model 3009 MP installed on Tricon V11.3.x systems that could cause module reset when TCM receives malformed TriStation packets while the write-protect keyswitch is in the program position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22744, CVE-2021-22745, and CVE-2021-22746.
CVE-2021-30193	2021-05-25	7.5		CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Write.
CVE-2021-30192	2021-05-25	7.5		CODESYS V2 Web-Server before 1.1.9.20 has an Improperly Implemented Security Check.
CVE-2021-30189	2021-05-25	7.5		CODESYS V2 Web-Server before 1.1.9.20 has a Stack-based Buffer Overflow.
CVE-2021-30190	2021-05-25	7.5		CODESYS V2 Web-Server before 1.1.9.20 has Improper Access Control.
CVE-2021-30188	2021-05-25	7.5		CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow.
CVE-2021-30194	2021-05-25	6.4		CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Read.
CVE-2021-30191	2021-05-25	5.0		CODESYS V2 Web-Server before 1.1.9.20 has a a Buffer Copy without Checking the Size of the Input.
CVE-2021-30195	2021-05-25	5.0		CODESYS V2 runtime system before 2.4.7.55 has Improper Input Validation.
CVE-2021-30186	2021-05-25	5.0		CODESYS V2 runtime system SP before 2.4.7.55 has a Heap-based Buffer Overflow.
CVE-2021-30187	2021-05-25	4.6		CODESYS V2 runtime system SP before 2.4.7.55 has Improper Neutralization of Special Elements used in an OS Command.
CVE-2021-27457	2021-05-20	5.0		A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access.
CVE-2020-20264	2021-05-19	4.0		Mikrotik RouterOs before 6.47 (stable tree) in the /ram/pckg/advanced-tools/nova/bin/netwatch process. An authenticated remote attacker can cause a Denial of Service due to a divide by zero error.
CVE-2020-20254	2021-05-18	4.0		Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).