Industrial Cybersecurity Center

ICS Vulnerabilities
CCI Thermometer
2021- 10

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.

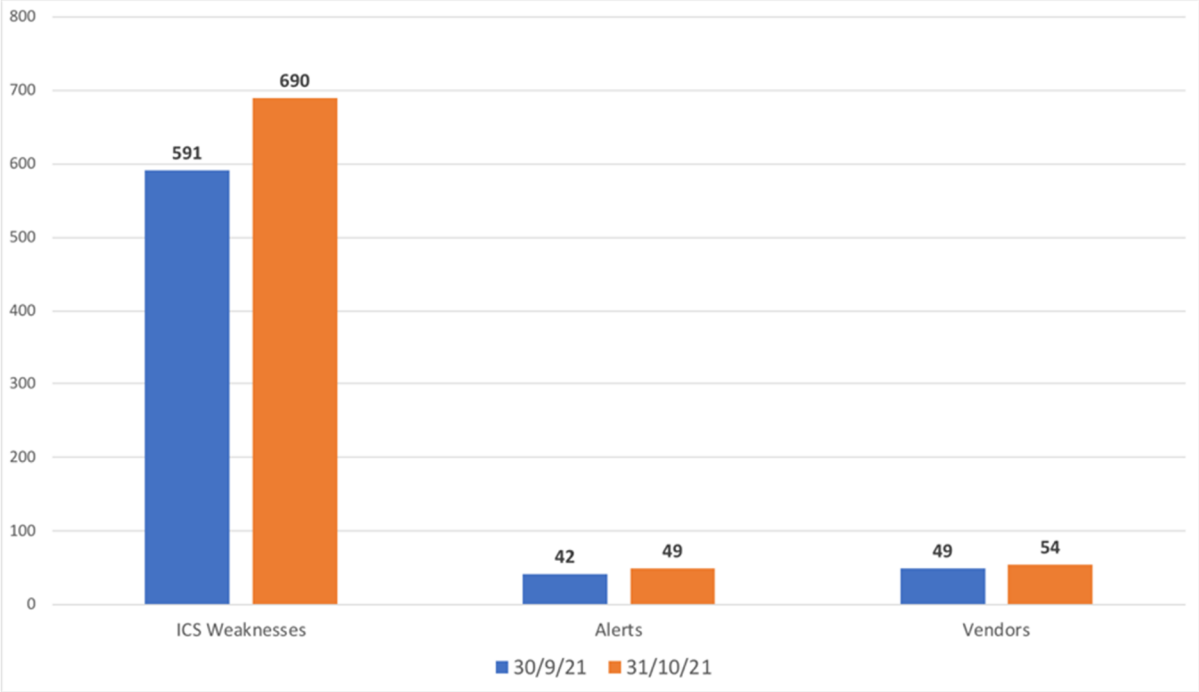
In each update we will publish:

- 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, **5** new **manufacturers** are included, and their number increases to **54** in 2021:

Low Risk	Medium Risk	High Risk	Very High Risk
LAquis SCADA Trane	Auvesy Hikvision	N/A	Dahua

Three of these manufacturers are in the original ICS-CERT set (**Trane**, **Hikvision** and **Dahua**).

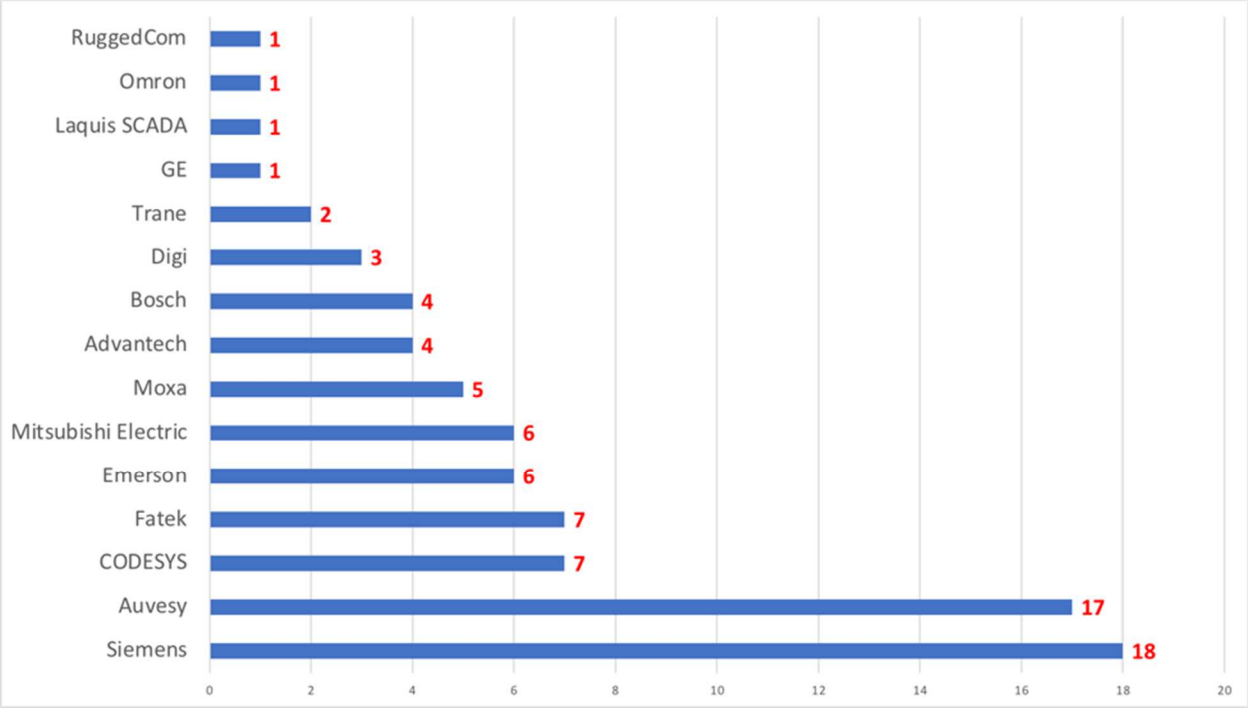
In the case of **LAquis**, the weaknesses are associated with its SCADA product and affect all versions up to 4.3.1.

The German manufacturer **Auvesy** enters the ICS-CERT and CCI list as it is a very widespread provider in all automation sectors with its Versiondog product for backing up field devices (PLCs, RTUs, etc.).
In this month of October, NIST has fully characterized **17 weaknesses** of its versiondog product, one of them being an alert (**CVE-2021-38475**)

New weaknesses

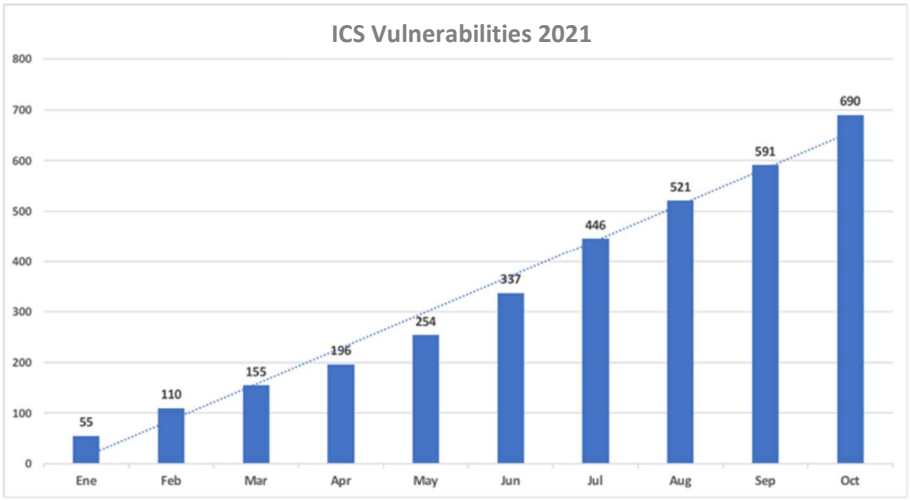
The number of ICS vulnerabilities published and **fully characterized** by NIST since the last update is **99**.

This month, the discovery of weaknesses is more distributed among manufacturers:



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

This third quarter 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) 7 new manufacturer alerts.

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).

Bosch Rexroth has seen 1 alert and 3 weaknesses published about its IndraMotion product:

Bosch Rexroth IndraMotion

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-23857	2021-10-04	10.0	⚠	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system.

The conjunction of these four weaknesses makes full access to the system possible:

CVE	Date published	CVSS V2	Vendor	Description
CVE-2021-23858	2021-10-04	7.8	Bosch	Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource.
CVE-2021-23855	2021-10-04	5.0	Bosch	The user and password data base is exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables.
CVE-2021-23856	2021-10-04	4.3	Bosch	The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client's computer by sending the client a manipulated URL.

In Auvesy's case, 16 weaknesses and 1 alert have been published by NIST this month about its versiondog product:

CVE	Date published	CVSS	Warning	Description
CVE-2021-38475	2021-10-22	9.0	⚠	The database connection to the server is performed by calling a specific API, which could allow an unprivileged user to gain SYSDBA permissions.

The problem is related to the injection of unauthenticated commands through its API. Given that it is the first time that this manufacturer enters the thermometer, and due to its wide implementation in the industrial sector, we detail the rest of the weaknesses found.

CVE	Date published	CVSS	Vendor	Description
CVE-2021-38449	2021-10-22	7.5	Auvesy	Some API functions permit by-design writing or copying data into a given buffer. Since the client controls these parameters, an attacker could rewrite the memory in any location of the affected product.
CVE-2021-38457	2021-10-22	7.5	Auvesy	The server permits communication without any authentication procedure, allowing the attacker to initiate a session with the server without providing any form of authentication.
CVE-2021-38459	2021-10-22	7.5	Auvesy	The data of a network capture of the initial handshake phase can be used to authenticate at a SYSDBA level. If a specific .exe is not restarted often, it is possible to access the needed handshake packets between admin/client connections. Using the SYSDBA permission, an attacker can change user passwords or delete the database.
CVE-2021-38481	2021-10-22	7.5	Auvesy	The scheduler service running on a specific TCP port enables the user to start and stop jobs. There is no sanitation of the supplied JOB ID provided to the function. An attacker may send a malicious payload that can enable the user to execute another SQL expression by sending a specific string.
CVE-2021-38473	2021-10-22	6.5	Auvesy	The affected product's code base doesn't properly control arguments for specific functions, which could lead to a stack overflow.
CVE-2021-38453	2021-10-22	6.4	Auvesy	Some API functions allow interaction with the registry, which includes reading values as well as data modification.
CVE-2021-38461	2021-10-22	6.4	Auvesy	The affected product uses a hard-coded blowfish key for encryption/decryption processes. The key can be easily extracted from binaries.
CVE-2021-38471	2021-10-22	6.4	Auvesy	There are multiple API function codes that permit data writing to any file, which may allow an attacker to modify existing files or create new files.
CVE-2021-38477	2021-10-22	6.4	Auvesy	There are multiple API function codes that permit reading and writing data to or from files and directories, which could lead to the manipulation and/or the deletion of files.
CVE-2021-38463	2021-10-22	5.5	Auvesy	The affected product does not properly control the allocation of resources. A user may be able to allocate unlimited memory buffers using API functions.

CVE	Date published	CVSS	Vendor	Description
CVE-2021-38467	2021-10-22	5.5	Auvesy	A specific function code receives a raw pointer supplied by the user and deallocates this pointer. The user can then control what memory regions will be freed and cause use-after-free condition.
CVE-2021-38479	2021-10-22	5.0	Auvesy	Many API function codes receive raw pointers remotely from the user and trust these pointers as valid in-bound memory regions. An attacker can manipulate API functions by writing arbitrary data into the resolved address of a raw pointer.
CVE-2021-38469	2021-10-22	4.3	Auvesy	Many of the services used by the affected product do not specify full paths for the DLLs they are loading. An attacker can exploit the uncontrolled search path by implanting their own DLL near the affected product's binaries, thus hijacking the loaded DLL.
CVE-2021-38455	2021-10-22	4.0	Auvesy	The affected product's OS Service does not verify any given parameter. A user can supply any type of parameter that will be passed to inner calls without checking the type of the parameter or the value.
CVE-2021-38465	2021-10-22	4.0	Auvesy	The webinstaller is a Golang web server executable that enables the generation of an Auvesy image agent. Resource consumption can be achieved by generating large amounts of installations, which are then saved without limitation in the temp folder of the webinstaller executable.
CVE-2021-38451	2021-10-22	3.5	Auvesy	The affected product's proprietary protocol CSC allows for calling numerous function codes. In order to call those function codes, the user must supply parameters. There is no sanitation on the value of the offset, which allows the client to specify any offset and read out-of-bounds data.

Siemens once again sees another weakness posted on a broad series of industrial level 3 routers and switches in its RuggedCom ROX family:

CVE	Date published	CVSS	Warning	Description
CVE-2021-41546	2021-10-12	7.8	⚠	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.14.1), RUGGEDCOM ROX RX1400 (All versions < V2.14.1), RUGGEDCOM ROX RX1500 (All versions < V2.14.1), RUGGEDCOM ROX RX1501 (All versions < V2.14.1), RUGGEDCOM ROX RX1510 (All versions < V2.14.1), RUGGEDCOM ROX RX1511 (All versions < V2.14.1), RUGGEDCOM ROX RX1512 (All versions < V2.14.1), RUGGEDCOM ROX RX1524 (All versions < V2.14.1), RUGGEDCOM ROX RX1536 (All versions < V2.14.1), RUGGEDCOM ROX RX5000 (All versions < V2.14.1). Affected devices write crashdumps without checking if enough space is available on the filesystem. Once the crashdump fills the entire root filesystem, affected devices fail to boot successfully. An attacker can leverage this vulnerability to cause a permanent Denial-of-Service.

Alerts have also been posted on various Siemens products used in different sectors. Specifically about your SINUMERIK 808D product and your SINEC NMS monitoring solution.

CVE	Date published	CVSS	Warning	Description
CVE-2021-33728	2021-10-12	9.0	⚠	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system allows to upload JSON objects that are deserialized to JAVA objects. Due to insecure deserialization of user-supplied content by the affected software, a privileged attacker could exploit this vulnerability by sending a crafted serialized Java object. An exploit could allow the attacker to execute arbitrary code on the device with root privileges.
CVE-2021-31891	2021-10-12	7.8	⚠	A vulnerability has been identified in SINUMERIK 808D (All versions), SINUMERIK 828D (All versions < V4.95). Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.

Phoenix Contact once again sees weaknesses classified as alerts published in its PLCNext family of products

CVE	Date published	CVSS	Warning	Description
CVE-2021-34570	2021-09-27	7.8	⚠	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.

In the case of Dahua, the alert characterized this month affects different security cameras produced by this manufacturer.

.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-33044	2021-09-15	10.0	⚠	The identity authentication bypass vulnerability found in some Dahua products during the login process. Attackers can bypass device identity authentication by constructing malicious data packets.

We must highlight the existence of public attacks on the Internet on this weakness, so we recommend updating the versions of these devices as soon as possible.

Risk map

October 31, 2021

	Circutor Delta Electronics	Dahua		
Digitek Hikvision Johnson Controls Motorola Solutions Pro-face Zebra Industrial	Advantech Auvesy B. Braun Medical Bosch Emerson Hilscher Miitsubishi Electric Morpho Moxa Panasonic Phoenix Contact RugggedCom Schneider Electric Wago			Siemens
ABB Beckhoff 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 National Instruments Philips ProSoft SafeNet SearchBlox Tesla Trane				

Changes in manufacturing risk

Emerson increases its exposure on the Risk Map with a **Medium +** value, due to the publication of 6 weaknesses. This manufacturer has seen 18 CVEs published in 2021 and its average CVSS V2 for the last 10 years is **5.4**.

RuggedCom rises on the risk map with a **Medium +** value, as for the second consecutive month an alert is published affecting its ROX family of products. Your average CVSS for the past 10 years is **5.8**.

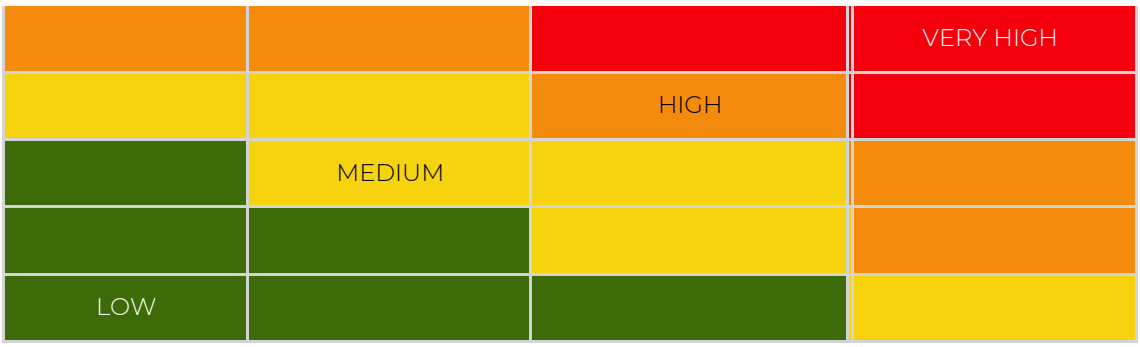
Dahua enters directly with a **Very High** risk due to the publication of a CVE (which is characterized as an alert) on its security cameras- The list of affected products is very long: IPC-X3XXX, HX5XXX, HUM7XX, VTO75X95X, VTO65XXX, VTH542XH, PTZ Dome Camera SD1A1, SD22, SD49, SD50, SD52C, SD6AL, Thermal TPC-BF1241, TPC-BF2221, TPC-SD2221, TPC-BF5XXX, TPC-SD8X21, TPC-PT8X21B, NVR1XXX, NVR2XXX, NVR4XXX, NVR6.
In addition, **there is a proof of concept published on the Internet** to attack these devices. Your average CVSS V2 for the last 10 years becomes **6.6**.

Hikvision suffers a similar behavior and enters the risk map with a Medium value. The published weakness is not characterized as elrta due to the characterization of the complexity of the network attack (Medium) and its average CVSS V2 of the last 10 years becomes **6.2**.

The rest of the manufacturers maintain their level in the qualitative heat map of risk exposure.

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-2021-38450	2021-10-27	6.5		The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software.
CVE-2021-38475	2021-10-22	9.0	⚠	The database connection to the server is performed by calling a specific API, which could allow an unprivileged user to gain SYSDBA permissions.
CVE-2021-23857	2021-10-04	10.0	⚠	Login with hash: The login routine allows the client to log in to the system not by using the password, but by using the hash of the password. Combined with CVE-2021-23858, this allows an attacker to subsequently login to the system.
CVE-2021-41546	2021-10-12	7.8	⚠	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.14.1), RUGGEDCOM ROX RX1400 (All versions < V2.14.1), RUGGEDCOM ROX RX1500 (All versions < V2.14.1), RUGGEDCOM ROX RX1501 (All versions < V2.14.1), RUGGEDCOM ROX RX1510 (All versions < V2.14.1), RUGGEDCOM ROX RX1511 (All versions < V2.14.1), RUGGEDCOM ROX RX1512 (All versions < V2.14.1), RUGGEDCOM ROX RX1524 (All versions < V2.14.1), RUGGEDCOM ROX RX1536 (All versions < V2.14.1), RUGGEDCOM ROX RX5000 (All versions < V2.14.1). Affected devices write crashdumps without checking if enough space is available on the filesystem. Once the crashdump fills the entire root filesystem, affected devices fail to boot successfully. An attacker can leverage this vulnerability to cause a permanent Denial-of-Service.
CVE-2021-33728	2021-10-12	9.0	⚠	A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system allows to upload JSON objects that are deserialized to JAVA objects. Due to insecure deserialization of user-supplied content by the affected software, a privileged attacker could exploit this vulnerability by sending a crafted serialized Java object. An exploit could allow the attacker to execute arbitrary code on the device with root privileges.
CVE-2021-31891	2021-10-12	7.8	⚠	A vulnerability has been identified in SINUMERIK 808D (All versions), SINUMERIK 828D (All versions < V4.95). Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.
CVE-2021-34570	2021-09-27	7.8	⚠	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.
CVE-2021-33044	2021-09-15	10.0	⚠	The identity authentication bypass vulnerability found in some Dahua products during the login process. Attackers can bypass device identity authentication by constructing malicious data packets.
CVE-2021-32951	2021-10-27	5.0		WebAccess/NMS (Versions prior to v3.0.3_Build6299) has an improper authentication vulnerability, which may allow unauthorized users to view resources monitored and controlled by the WebAccess/NMS, as well as IP addresses and names of all the devices managed via WebAccess/NMS.
CVE-2021-34584	2021-10-26	6.4		Crafted web server requests can be utilised to read partial stack or heap memory or may trigger a denial-of- service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22.
CVE-2021-34595	2021-10-26	5.5		A crafted request with invalid offsets may cause an out-of-bounds read or write access in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition or local memory overwrite.
CVE-2021-34593	2021-10-26	5.0		In CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56 unauthenticated crafted invalid requests may result in several denial-of-service conditions. Running PLC programs may be stopped, memory may be leaked, or further communication clients may be blocked from accessing the PLC.
CVE-2021-34586	2021-10-26	5.0		In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests may cause a Null pointer dereference in the CODESYS web server and may result in a denial-of-service condition.
CVE-2021-34585	2021-10-26	5.0		In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests can trigger a parser error. Since the parser result is not checked under all conditions, a pointer dereference with an invalid address can occur. This leads to a denial of service situation.
CVE-2021-34583	2021-10-26	5.0		Crafted web server requests may cause a heap-based buffer overflow and could therefore trigger a denial-of- service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-34596	2021-10-26	4.0		A crafted request may cause a read access to an uninitialized pointer in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition.
CVE-2021-38457	2021-10-22	7.5		The server permits communication without any authentication procedure, allowing the attacker to initiate a session with the server without providing any form of authentication.
CVE-2021-38481	2021-10-22	7.5		The scheduler service running on a specific TCP port enables the user to start and stop jobs. There is no sanitation of the supplied JOB ID provided to the function. An attacker may send a malicious payload that can enable the user to execute another SQL expression by sending a specific string.
CVE-2021-38459	2021-10-22	7.5		The data of a network capture of the initial handshake phase can be used to authenticate at a SYSDBA level. If a specific .exe is not restarted often, it is possible to access the needed handshake packets between admin/client connections. Using the SYSDBA permission, an attacker can change user passwords or delete the database.
CVE-2021-38449	2021-10-22	7.5		Some API functions permit by-design writing or copying data into a given buffer. Since the client controls these parameters, an attacker could rewrite the memory in any location of the affected product.
CVE-2021-38485	2021-10-22	6.5		The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk.
CVE-2021-42542	2021-10-22	6.5		The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure.
CVE-2021-42540	2021-10-22	6.5		The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality.
CVE-2021-42538	2021-10-22	6.5		The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input.
CVE-2021-42539	2021-10-22	6.5		The affected product is vulnerable to a missing permission validation on system backup restore, which could lead to account take over and unapproved settings change.
CVE-2021-38473	2021-10-22	6.5		The affected product's code base doesn't properly control arguments for specific functions, which could lead to a stack overflow.
CVE-2021-38477	2021-10-22	6.4		There are multiple API function codes that permit reading and writing data to or from files and directories, which could lead to the manipulation and/or the deletion of files.
CVE-2021-38471	2021-10-22	6.4		There are multiple API function codes that permit data writing to any file, which may allow an attacker to modify existing files or create new files.
CVE-2021-38461	2021-10-22	6.4		The affected product uses a hard-coded blowfish key for encryption/decryption processes. The key can be easily extracted from binaries.
CVE-2021-38453	2021-10-22	6.4		Some API functions allow interaction with the registry, which includes reading values as well as data modification.
CVE-2021-38463	2021-10-22	5.5		The affected product does not properly control the allocation of resources. A user may be able to allocate unlimited memory buffers using API functions.
CVE-2021-38467	2021-10-22	5.5		A specific function code receives a raw pointer supplied by the user and deallocates this pointer. The user can then control what memory regions will be freed and cause use-after-free condition.
CVE-2021-38479	2021-10-22	5.0		Many API function codes receive raw pointers remotely from the user and trust these pointers as valid in-bound memory regions. An attacker can manipulate API functions by writing arbitrary data into the resolved address of a raw pointer.
CVE-2021-42534	2021-10-22	4.3		The affected product's web application does not properly neutralize the input during webpage generation, which could allow an attacker to inject code in the input forms.
CVE-2021-38469	2021-10-22	4.3		Many of the services used by the affected product do not specify full paths for the DLLs they are loading. An attacker can exploit the uncontrolled search path by implanting their own DLL near the affected product's binaries, thus hijacking the loaded DLL.
CVE-2021-42536	2021-10-22	4.0		The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables.
CVE-2021-38465	2021-10-22	4.0		The webinstaller is a Golang web server executable that enables the generation of an Auvesy image agent. Resource consumption can be achieved by generating large amounts of installations, which are then saved without limitation in the temp folder of the webinstaller executable.
CVE-2021-38455	2021-10-22	4.0		The affected product's OS Service does not verify any given parameter. A user can supply any type of parameter that will be passed to inner calls without checking the type of the parameter or the value.
CVE-2021-38451	2021-10-22	3.5		The affected product's proprietary protocol CSC allows for calling numerous function codes. In order to call those function codes, the user must supply parameters. There is no sanitation on the value of the offset, which allows the client to specify any offset and read out-of-bounds data.
CVE-2020-23058	2021-10-22	2.1		An issue in the authentication mechanism in Nong Ge File Explorer v1.4 unauthenticated allows to access sensitive data.
CVE-2021-20836	2021-10-19	6.0		Out-of-bounds read vulnerability in CX-Supervisor v4.0.0.13 and v4.0.0.16 allows an attacker with administrative privileges to cause information disclosure and/or arbitrary code execution by opening a specially crafted SCS project files.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-38389	2021-10-18	7.5		Advantech WebAccess versions 9.02 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute code.
CVE-2021-33023	2021-10-18	7.5		Advantech WebAccess versions 9.02 and prior are vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute code.
CVE-2021-38430	2021-10-18	6.8		FATEK Automation WinProladder versions 3.30 and prior proper validation of user-supplied data when parsing project files, which could result in a stack-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code.
CVE-2021-38434	2021-10-18	6.8		FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in an unexpected sign extension. An attacker could leverage this vulnerability to execute arbitrary code.
CVE-2021-38426	2021-10-18	6.8		FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code.
CVE-2021-38436	2021-10-18	6.8		FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in a memory-corruption condition. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.
CVE-2021-38442	2021-10-18	6.8		FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in a heap-corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process.
CVE-2021-38438	2021-10-18	6.8		A use after free vulnerability in FATEK Automation WinProladder versions 3.30 and prior may be exploited when a valid user opens a malformed project file, which may allow arbitrary code execution.
CVE-2021-38440	2021-10-18	4.3		FATEK Automation WinProladder versions 3.30 and prior is vulnerable to an out-of-bounds read, which may allow an attacker to read unauthorized information.
CVE-2021-38432	2021-10-15	7.5		FATEK Automation Communication Server Versions 1.13 and prior lacks proper validation of user-supplied data, which could result in a stack-based buffer overflow condition and allow an attacker to remotely execute code.
CVE-2018-16060	2021-10-15	5.0		Mitsubishi Electric SmartRTU devices allow remote attackers to obtain sensitive information (directory listing and source code) via a direct request to the /web URI.
CVE-2018-16061	2021-10-15	4.3		Mitsubishi Electric SmartRTU devices allow XSS via the username parameter or PATH_INFO to login.php.
CVE-2021-38431	2021-10-15	4.0		An authenticated user using Advantech WebAccess SCADA in versions 9.0.3 and prior can use API functions to disclose project names and paths from other users.
CVE-2021-20599	2021-10-14	5.0		Authorization bypass through user-controlled key vulnerability in MELSEC iQ-R series Safety CPU R08/16/32/120SFCPU all versions and MELSEC iQ-R series SIL2 Process CPU R08/16/32/120PSFCPU all versions allows an remote unauthenticated attacker to login to a target CPU module by obtaining credentials other than password.
CVE-2021-38456	2021-10-12	7.5		A use of hard-coded password vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to gain access through accounts using default passwords
CVE-2021-38454	2021-10-12	7.5		A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.
CVE-2021-38458	2021-10-12	7.5		A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.
CVE-2021-33729	2021-10-12	6.5		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). An authenticated attacker that is able to import firmware containers to an affected system could execute arbitrary commands in the local database.
CVE-2021-33730	2021-10-12	6.5		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). A privileged authenticated attacker could execute arbitrary commands in the local database by sending crafted requests to the webserver of the affected application.
CVE-2021-38452	2021-10-12	6.4		A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.
CVE-2021-27395	2021-10-12	5.5		A vulnerability has been identified in SIMATIC Process Historian 2013 and earlier (All versions), SIMATIC Process Historian 2014 (All versions < SP3 Update 6), SIMATIC Process Historian 2019 (All versions), SIMATIC Process Historian 2020 (All versions). An interface in the software that is used for critical functionalities lacks authentication, which could allow a malicious user to maliciously insert, modify or delete data.
CVE-2021-33724	2021-10-12	5.0		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system contains an Arbitrary File Deletion vulnerability that possibly allows to delete an arbitrary file or directory under a user controlled path.
CVE-2021-33726	2021-10-12	5.0		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system allows to download arbitrary files under a user controlled path and does not correctly check if the relative path is still within the intended target directory.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-33725	2021-10-12	5.0		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system allows to delete arbitrary files or directories under a user controlled path and does not correctly check if the relative path is still within the intended target directory.
CVE-2021-38460	2021-10-12	5.0		A path traversal vulnerability in the Moxa MXview Network Management software Versions 3.x to 3.2.2 may allow an attacker to create or overwrite critical files used to execute code, such as programs or libraries.
CVE-2021-33722	2021-10-12	4.0		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). The affected system has a Path Traversal vulnerability when exporting a firmware container. With this a privileged authenticated attacker could create arbitrary files on an affected system.
CVE-2021-33727	2021-10-12	4.0		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). An authenticated attacker could download the user profile of any user. With this, the attacker could leak confidential information of any user in the affected system.
CVE-2021-33723	2021-10-12	4.0		A vulnerability has been identified in SINEC NMS (All versions < V1.0 SP2 Update 1). An authenticated attacker could change the user profile of any user without proper authorization. With this, the attacker could change the password of any user in the affected system.
CVE-2021-36767	2021-10-08	7.5		In Digi RealPort through 4.8.488.0, authentication relies on a challenge-response mechanism that gives access to the server password, making the protection ineffective. An attacker may send an unauthenticated request to the server. The server will reply with a weakly-hashed version of the server's access password. The attacker may then crack this hash offline in order to successfully login to the server.
CVE-2021-35977	2021-10-08	7.5		An issue was discovered in Digi RealPort for Windows through 4.8.488.0. A buffer overflow exists in the handling of ADDP discovery response messages. This could result in arbitrary code execution.
CVE-2021-35979	2021-10-08	6.8		An issue was discovered in Digi RealPort through 4.8.488.0. The 'encrypted' mode is vulnerable to man-in-the-middle attacks and does not perform authentication.
CVE-2021-20600	2021-10-08	4.3		Uncontrolled resource consumption in MELSEC iQ-R series C Controller Module R12CCPU-V all versions allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending a large number of packets in a short time while the module starting up.
CVE-2021-20603	2021-10-07	5.0		Improper Input Validation vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets.
CVE-2021-20602	2021-10-07	5.0		Improper Handling of Exceptional Conditions vulnerability in GOT2000 series GT21 model GT2107-WTBD all versions, GT2107-WTSD all versions, GT2104-RTBD all versions, GT2104-PMBD all versions, GT2103-PMBD all versions, GOT SIMPLE series GS21 model GS2110-WTBD all versions, GS2107-WTBD all versions, GS2110-WTBD-N all versions, GS2107-WTBD-N all versions and LE7-40GU-L all versions allows a remote unauthenticated attacker to cause DoS condition of the products by sending specially crafted packets.
CVE-2021-23858	2021-10-04	7.8		Information disclosure: The main configuration, including users and their hashed passwords, is exposed by an unprotected web server resource and can be accessed without authentication. Additionally, device details are exposed which include the serial number and the firmware version by another unprotected web server resource.
CVE-2021-41579	2021-10-04	6.8		LCDS LAquis SCADA through 4.3.1.1085 is vulnerable to a control bypass and path traversal. If an attacker can get a victim to load a malicious els project file and use the play feature, then the attacker can bypass a consent popup and write arbitrary files to OS locations where the user has permission, leading to code execution.
CVE-2021-23855	2021-10-04	5.0		The user and password data base is exposed by an unprotected web server resource. Passwords are hashed with a weak hashing algorithm and therefore allow an attacker to determine the password by using rainbow tables.
CVE-2021-23856	2021-10-04	4.3		The web server is vulnerable to reflected XSS and therefore an attacker might be able to execute scripts on a client’s computer by sending the client a manipulated URL.
CVE-2020-12030	2021-09-29	6.8		There is a flaw in the code used to configure the internal gateway firewall when the gateway's VLAN feature is enabled. If a user enables the VLAN setting, the internal gateway firewall becomes disabled resulting in exposure of all ports used by the gateway.
CVE-2021-41537	2021-09-28	6.8		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13789).
CVE-2021-41536	2021-09-28	6.8		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13778).
CVE-2021-41540	2021-09-28	6.8		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An

CVE	Date published	CVSS V2	Warning	Description
				attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13776).
CVE-2021-41539	2021-09-28	6.8		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13773).
CVE-2021-41535	2021-09-28	6.8		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13771).
CVE-2021-41538	2021-09-28	4.3		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ files. An attacker could leverage this vulnerability to leak information from unexpected memory locations (ZDI-CAN-13770).
CVE-2021-41534	2021-09-28	4.3		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13703).
CVE-2021-41533	2021-09-28	4.3		A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13565).
CVE-2021-22272	2021-09-27	9.0		The vulnerability origins in the commissioning process where an attacker of the ControlTouch can enter a serial number in a specific way to transfer the device virtually into her/his my.busch-jaeger.de or mybuildings.abb.com profile. A successful attacker can observe and control a ControlTouch remotely under very specific circumstances. The issue is fixed in the cloud side of the system. No firmware update is needed for customer products. If a user wants to understand if (s)he is affected, please read the advisory. This issue affects: ABB and Busch-Jaeger, ControlTouch
CVE-2021-32959	2021-09-23	7.5		Heap-based buffer overflow in SuiteLink server while processing commands 0x05/0x06
CVE-2021-32979	2021-09-23	5.0		Null pointer dereference in SuiteLink server while processing commands 0x04/0x0a
CVE-2021-32963	2021-09-23	5.0		Null pointer dereference in SuiteLink server while processing commands 0x03/0x10
CVE-2021-32987	2021-09-23	5.0		Null pointer dereference in SuiteLink server while processing command 0x0b
CVE-2021-32971	2021-09-23	5.0		Null pointer dereference in SuiteLink server while processing command 0x07
CVE-2021-32999	2021-09-23	5.0		Improper handling of exceptional conditions in SuiteLink server while processing command 0x01
CVE-2021-22276	2021-09-23	4.3		The vulnerability allows a successful attacker to bypass the integrity check of FW uploaded to the free@home System Access Point.
CVE-2021-36260	2021-09-22	9.3		A command injection vulnerability in the web server of some Hikvision product. Due to the insufficient input validation, attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.