Industrial Cybersecurity
Center

ICS Vulnerabilities
CCI Thermometer
2021- 3

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 5
New alerts 6
Risk map 7
Changes in manufacturing risk 7
ANNEX – I: Risk map calculation 9
ANNEX II – Vulnerabilities published by NIST since the last CCI Thermometer 10

Industrial Cybersecurity profesional 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**.

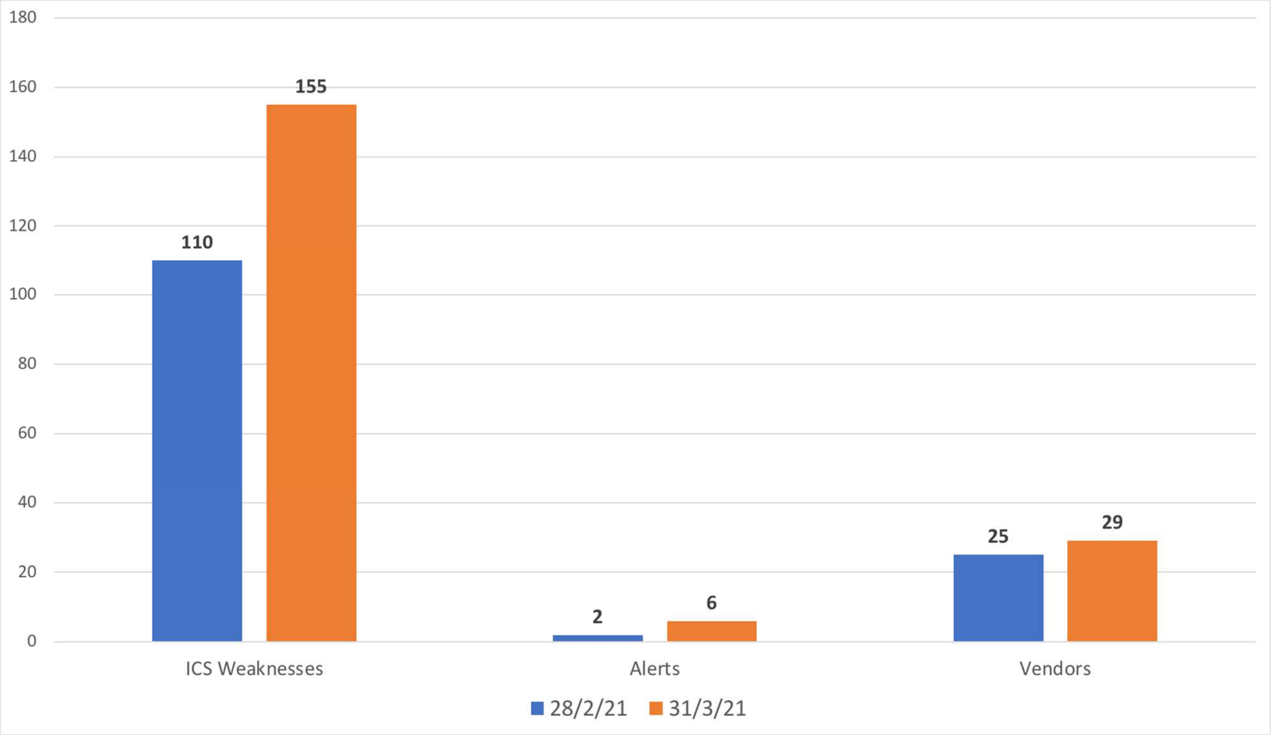
In each update we will publish:

- **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, the following **4 manufacturers** are included:

Low Risk	Medium Risk	High Risk	Very High Risk
Fatek ProSoft RuggedCom	Mitsubishi Electric	N/A	N/A

New weaknesses

The number of ICS vulnerabilities released by NIST since the last update is **45**.

Siemens is the manufacturer that accumulates the most weaknesses published in March 2021 **(14 CVEs)** and continues to lead the risk map for 2021 together with Panasonic.

Advantech also increases its risk level by having **5 CVEs** published in the month of March.

The average monthly rate of ICS weakness discovery remains around 50, so that the year 2021 could set a new record.

New alerts

This month, **NIST** has released **4** 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.

CVE	Date published	CVSS	Warning	Description
CVE-2021-27221	2021-03-19	8.5	⚠	** DISPUTED ** MikroTik RouterOS 6.47.9 allows remote authenticated ftp users to create or overwrite arbitrary .rsc files via the /export command. NOTE: the vendor's position is that this is intended behavior because of how user policies work.
CVE-2020-19417	2021-03-10	9.0	⚠	Emerson Smart Wireless Gateway 1420 4.6.59 allows non-privileged users (such as the default account 'maint') to perform administrative tasks by sending specially crafted HTTP requests to the application.
CVE-2021-22667	2021-02-24	10.0	⚠	BB-ESWGP506-2SFP-T versions 1.01.09 and prior is vulnerable due to the use of hard-coded credentials, which may allow an attacker to gain unauthorized access and permit the execution of arbitrary code on the BB-ESWGP506-2SFP-T (versions 1.01.01 and prior).
CVE-2021-27452	2021-03-25	10.0	⚠	The software contains a hard-coded password that could allow an attacker to take control of the merging unit using these hard-coded credentials on the MU320E (all firmware versions prior to v04A00.1).

MikroTik RouterOS

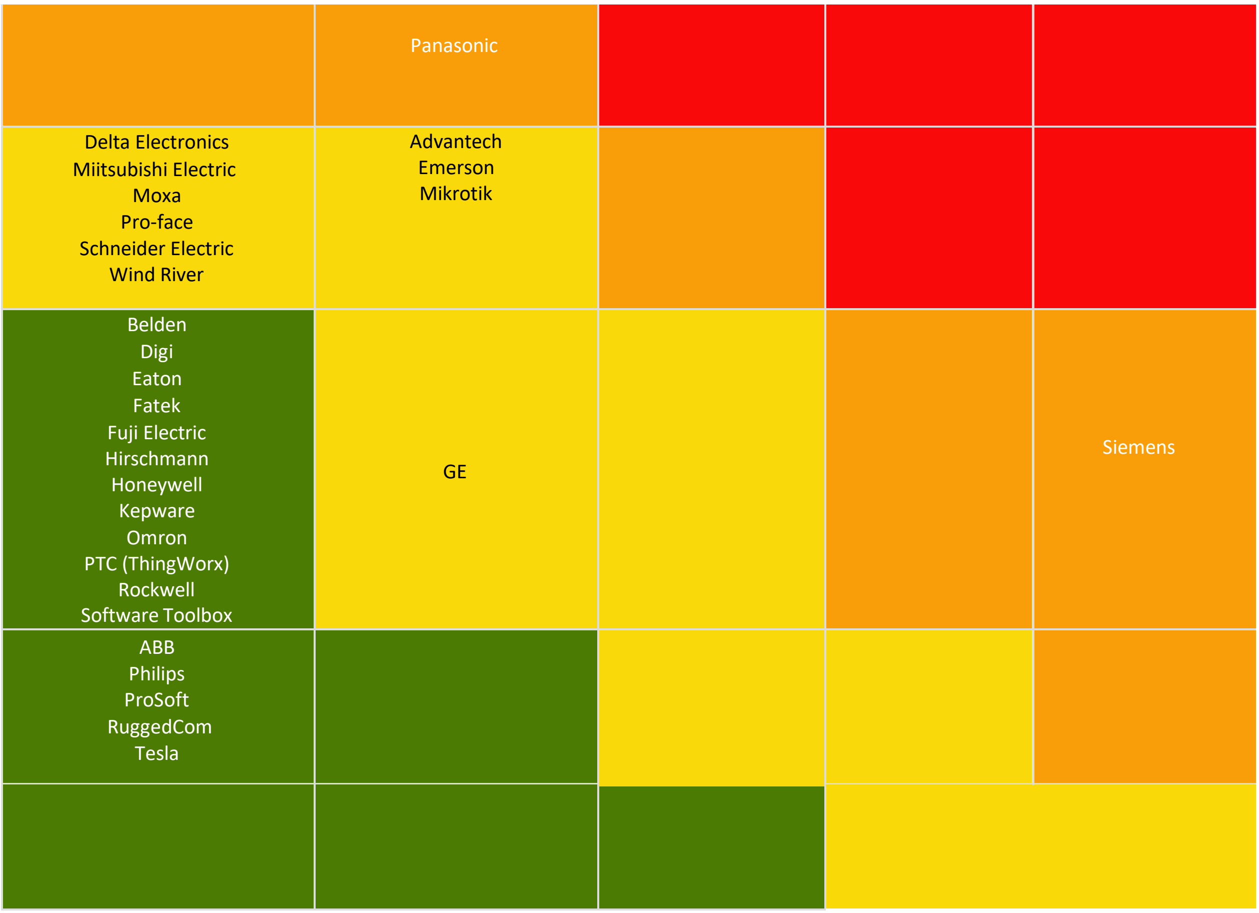
Emerson Smart Wireless Gateway 1420

Advantech BB-ESWGP506-2SFP-T

GE MU320

Risk map

March 31, 2021



	Panasonic			
Delta Electronics Miitsubishi Electric Moxa Pro-face Schneider Electric Wind River	Advantech Emerson Mikrotik			
Belden Digi Eaton Fatek Fuji Electric Hirschmann Honeywell Kepware Omron PTC (ThingWorx) Rockwell Software Toolbox	GE			Siemens
ABB Philips ProSoft RuggedCom Tesla				

Changes in manufacturing risk

4 new manufacturers are incorporated:

- Fatek, ProSoft and RuggedCom with **Low** risk.
- Mitsubishi Electric with **Medium** risk.

Advantech, Emerson, GE and MikroTik increase their risk position on the map (Medium Risk), after 1 alert from each manufacturer was published by NIST in March 2021.

Advantech currently counts **16** CVEs in 2021 with an average CVSS V2 of **6.9** over the last 10 years. Emerson accumulates **3** CVEs in 2021 with an average CVSS V2 of **6.4** in the last 10 years and MikroTik closes with 2 CVEs in 2021 and an average CVSS V2 of 6.2 in the last 10 years.

In the case of Misubishi Electric, **2** CVEs published in March affect a large number of equipment from this manufacturer (CVE-2021-20587 y CVE-2021-20588), and assign it an average CVSS V2 of 6.6 in the last 10 years.

GE counts **8** vulnerabilities published by NIST in 2021, and in this month of March the 3 vulnerabilities published on one of its products (MU320E), of which 1 is an alert, make it increase its position on the risk map. GE thus obtains an average CVSS V2 of 7.5 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.

🟧	🟧	🟥	🟥	🟥 VERY HIGH
🟨	🟨	🟧 HIGH	🟥	🟥
🟩	🟨 MEDIUM	🟨	🟧	🟧
🟩	🟩	🟨	🟨	🟧
🟩 LOW	🟩	🟩	🟨	🟨

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-2021-27221	2021-03-19	8.5	⚠	** DISPUTED ** MikroTik RouterOS 6.47.9 allows remote authenticated ftp users to create or overwrite arbitrary .rsc files via the /export command. NOTE: the vendor's position is that this is intended behavior because of how user policies work.
CVE-2021-27452	2021-03-25	10.0	⚠	The software contains a hard-coded password that could allow an attacker to take control of the merging unit using these hard-coded credentials on the MU320E (all firmware versions prior to v04A00.1).
CVE-2021-27450	2021-03-25	4.6		SSH server configuration file does not implement some best practices. This could lead to a weakening of the SSH protocol strength, which could lead to additional misconfiguration or be leveraged as part of a larger attack on the MU320E (all firmware versions prior to v04A00.1).
CVE-2021-27448	2021-03-25	4.6		A miscommunication in the file system allows adversaries with access to the MU320E to escalate privileges on the MU320E (all firmware versions prior to v04A00.1).
CVE-2021-22665	2021-03-18	7.2		Rockwell Automation DriveTools SP v5.13 and below and Drives AOP v4.12 and below both contain a vulnerability that a local attacker with limited privileges may be able to exploit resulting in privilege escalation and complete control of the system.
CVE-2020-14516	2021-03-18	7.5		In Rockwell Automation FactoryTalk Services Platform Versions 6.10.00 and 6.11.00, there is an issue with the implementation of the SHA-256 hashing algorithm with FactoryTalk Services Platform that prevents the user password from being hashed properly.
CVE-2021-27436	2021-03-18	4.3		WebAccess/SCADA Versions 9.0 and prior is vulnerable to cross-site scripting, which may allow an attacker to send malicious JavaScript code to an unsuspecting user, which could result in hijacking of the user’s cookie/session tokens, redirecting the user to a malicious webpage and performing unintended browser actions.
CVE-2019-18231	2021-03-17	5.0		Advantech Spectre RT ERT351 Versions 5.1.3 and prior logins and passwords are transmitted in clear text form, which may allow an attacker to intercept the request.
CVE-2019-18233	2021-03-17	4.3		In Advantech Spectre RT Industrial Routers ERT351 5.1.3 and prior, the affected product does not neutralize special characters in the error response, allowing attackers to use a reflected XSS attack.
CVE-2019-18235	2021-03-17	7.5		Advantech Spectre RT ERT351 Versions 5.1.3 and prior has insufficient login authentication parameters required for the web application may allow an attacker to gain full access using a brute-force password attack.
CVE-2020-25236	2021-03-15	4.9		A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). The control logic (CL) the LOGO! 8 executes could be manipulated in a way that could cause the device executing the CL to improperly handle the manipulation and crash. After successful execution of the attack, the device needs to be manually reset.
CVE-2020-25239	2021-03-15	6.5		A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0). The webserver could allow unauthorized actions via special urls for unpriviledged users. The settings of the UMC authorization server could be changed to add a rogue server by an attacker authenticating with unprivilege user rights.
CVE-2020-25240	2021-03-15	6.5		A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0). Unpriviledged users can access services when guessing the url. An attacker could impact availability, integrity and gain information from logs and

CVE	Date published	CVSS V2	Warning	Description
				templates of the service.
CVE-2020-25241	2021-03-15	5.0		A vulnerability has been identified in SIMATIC MV400 family (All Versions < V7.0.6). The underlying TCP stack of the affected products does not correctly validate the sequence number for incoming TCP RST packages. An attacker could exploit this to terminate arbitrary TCP sessions.
CVE-2020-28385	2021-03-15	6.8		A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP3), Solid Edge SE2021 (SE2021MP3). Affected applications 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. (ZDI-CAN-12049)
CVE-2020-28387	2021-03-15	4.3		A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP3). When opening a specially crafted SEECTCXML file, the application could disclose arbitrary files to remote attackers. This is because of the passing of specially crafted content to the underlying XML parser without taking proper restrictions such as prohibiting an external dtd. (ZDI-CAN-11923)
CVE-2021-25667	2021-03-15	5.8		A vulnerability has been identified in RUGGEDCOM RM1224 (All versions >= V4.3), SCALANCE M-800 (All versions >= V4.3), SCALANCE S615 (All versions >= V4.3), SCALANCE SC-600 Family (All versions >= V2.0 and < V2.1.3), SCALANCE X300WG (All versions < V4.1), SCALANCE XM400 (All versions < V6.2), SCALANCE XR500 (All versions < V6.2), SCALANCE Xx200 Family (All versions < V4.1). Affected devices contain a stack-based buffer overflow vulnerability in the handling of STP BPDU frames that could allow a remote attacker to trigger a denial-of-service condition or potentially remote code execution. Successful exploitation requires the passive listening feature of the device to be active.
CVE-2021-25673	2021-03-15	4.9		A vulnerability has been identified in SIMATIC S7-PLCSIM V5.4 (All versions). An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, the application could enter an infinite loop, become unresponsive and must be restarted to restore the service.
CVE-2021-25674	2021-03-15	2.1		A vulnerability has been identified in SIMATIC S7-PLCSIM V5.4 (All versions). An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, a NULL pointer deference condition could cause the application to terminate unexpectedly and must be restarted to restore the service.
CVE-2021-25675	2021-03-15	2.1		A vulnerability has been identified in SIMATIC S7-PLCSIM V5.4 (All versions). An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, a divide by zero operation could occur and cause the application to terminate unexpectedly and must be restarted to restore the service.
CVE-2021-25676	2021-03-15	5.0		A vulnerability has been identified in RUGGEDCOM RM1224 (V6.3), SCALANCE M-800 (V6.3), SCALANCE S615 (V6.3), SCALANCE SC-600 (All Versions >= V2.1 and < V2.1.3). Multiple failed SSH authentication attempts could trigger a temporary Denial-of-Service under certain conditions. When triggered, the device will reboot automatically.
CVE-2021-27380	2021-03-15	6.8		A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP3), Solid Edge SE2021 (SE2021MP3). Affected applications lack proper validation of user-supplied data when parsing PAR 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-12532)

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-27381	2021-03-15	6.8		A vulnerability has been identified in Solid Edge SE2020 (All Versions < SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP3). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds read 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-12534)
CVE-2016-20009	2021-03-11	7.5		** UNSUPPORTED WHEN ASSIGNED ** A DNS client stack-based buffer overflow in ipdnsc_decode_name() affects Wind River VxWorks 6.5 through 7. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2021-22709	2021-03-11	9.3		A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in loss of data or remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.
CVE-2021-22710	2021-03-11	9.3		A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could cause remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.
CVE-2021-22711	2021-03-11	9.3		A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to missing validation of input data.
CVE-2021-22712	2021-03-11	9.3		A CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Interactive Graphical SCADA System (IGSS) Definition (Def.exe) V15.0.0.21041 and prior, which could result in arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to an unchecked pointer address.
CVE-2020-19417	2021-03-10	9.0	⚠	Emerson Smart Wireless Gateway 1420 4.6.59 allows non-privileged users (such as the default account 'maint') to perform administrative tasks by sending specially crafted HTTP requests to the application.
CVE-2020-19419	2021-03-10	5.0		Incorrect Access Control in Emerson Smart Wireless Gateway 1420 4.6.59 allows remote attackers to obtain sensitive device information from the administrator console without authentication.
CVE-2020-27632	2021-03-10	5.0		In SIMATIC MV400 family versions prior to v7.0.6, the ISN generator is initialized with a constant value and has constant increments. An attacker could predict and hijack TCP sessions.
CVE-2020-13554	2021-03-03	7.2		An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In webvrpcs Run Key Privilege Escalation in installation folder of WebAccess, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.
CVE-2021-22638	2021-03-03	6.8		Fatek FvDesigner Version 1.5.76 and prior is vulnerable to an out-of-bounds read while processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.
CVE-2021-22662	2021-03-03	6.8		A use after free issue has been identified in Fatek FvDesigner Version 1.5.76 and prior in the way the application processes project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.
CVE-2021-22666	2021-03-03	6.8		Fatek FvDesigner Version 1.5.76 and prior is vulnerable to a stack-based buffer overflow while project files are being processed, allowing an attacker to craft a special project file that may permit arbitrary code execution.
CVE-2021-22670	2021-03-03	6.8		An uninitialized pointer may be exploited in Fatek FvDesigner

CVE	Date published	CVSS V2	Warning	Description
				Version 1.5.76 and prior while the application is processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.
CVE-2021-22681	2021-03-03	7.5		Rockwell Automation Studio 5000 Logix Designer Versions 21 and later, and RSLogix 5000 Versions 16 through 20 use a key to verify Logix controllers are communicating with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800. Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20 are vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Rockwell Automation CompactLogix 1768, 1769, 5370, 5380, 5480: ControlLogix 5550, 5560, 5570, 5580; DriveLogix 5560, 5730, 1794-L34; Compact GuardLogix 5370, 5380; GuardLogix 5570, 5580; SoftLogix 5800.
CVE-2021-22683	2021-03-03	6.8		Fatek FvDesigner Version 1.5.76 and prior is vulnerable to an out-of-bounds write while processing project files, allowing an attacker to craft a special project file that may permit arbitrary code execution.
CVE-2021-22667	2021-02-24	10.0	⚠	BB-ESWGP506-2SFP-T versions 1.01.09 and prior is vulnerable due to the use of hard-coded credentials, which may allow an attacker to gain unauthorized access and permit the execution of arbitrary code on the BB-ESWGP506-2SFP-T (versions 1.01.01 and prior).