VERVE

A ROCKWELL AUTOMATION COMPANY

2022 CISA ICS Advisory Report

VERVE INDUSTRIAL'S ANNUAL REVIEW OF CISA ICS ADVISORIES - INTRODUCTION

Verve Industrial's mission is to help industrial clients ensure the security and reliability of their most critical assets: their industrial control systems. Verve brings over 25 years of ICS/OT controls experience to help clients achieve rapid and lasting improvement in their Operational Technology (OT) security.

Our foundation in industrial controls engineering is core to our mission to help operators protect these critical assets that keep modern civilization operating effectively. We act as a true partner to our clients in their security and reliability journey. We walk alongside our clients to help them increase the maturity of their systems and processes over time.

One of the key challenges our clients face is the flood of new ICS vulnerabilities released each year for ICS. They are often overwhelmed by the scale of these emerging risks. Our goal with this analysis is to bring some clarity to the task at hand, some visibility into the types of threats, and some recommendations about what actions an organization can take to address these risks.

2022 was another challenging year for people – after years of the [still ongoing] COVID-19 pandemic, tensions in the east ended up breaking into a full-fledged war, multiple industry verticals started to suffer the weight of an incoming recession (50% chance of a recession in 2023 according to the Guardian), and the number of hackers did nothing but increase.

During that year, and with the fact that the political landscape was all over the place, multiple threat actors used the opportunity to launch attacks on critical infrastructure and IACS. 2022 saw various groups – such as the Conti group – increase their number of attacks on industrial & automation control systems (IACS) and industrial/operational sectors such as energy, healthcare, etc.

On the other hand, positive events did happen in 2022 when it comes to cybersecurity – Multiple bills were passed by governments across the globe (e.g. USA, Canada) in order to improve the overall security of critical sectors.

To provide more information on the threat landscape for ICS, Verve's research team updated the analytical comparison completed last year regarding the trend of ICS advisories and CVEs.

To get a better view of growing ICS risks and vulnerabilities, Verve analyzed publicly available data points and reviewed our own vulnerability analysis data from the past couple of years. We:

- Examined the 370 ICS-CERT advisories for 2022 and extracted key insights
- Compared all the advisories from 2022 with the ones from past years (With a particular focus on 2021)
- Assessed the potential implications of those advisories
- Identified a few advisories that stand out from the pack
- Developed a list of recommendations for ICS staff based on our observations

Importantly, this analysis focuses on the specific ICS-advisories issued by CISA. These relate to hardware, firmware, and application software provided by ICS vendors to their critical infrastructure clients. Explicitly, this excludes the thousands of critical ICS vulnerabilities on the Windows OS and IT-type networking devices found in these same ICS environments. Those vulnerabilities are issued through traditional Vulnerability Management channels but have significant impact on ICS/OT environments.

Some ICS analysts make the argument that vulnerability and patch management is less important in OT than in IT because so few of the ICS advisories have a known exploit available. This is a misleading comment as the Windows, networking and other vulnerabilities on the HMIs, workstations, servers, switches and firewalls all have hundreds or thousands of vulnerabilities where a known exploit exists. And in most ICS environments, traditional IT patch and vulnerability management solutions are not feasible. Accurate vulnerability identification and efficient patch management is critically important for ICS.

ICS vulnerabilities provided in those advisories do not provide a comprehensive threat landscape as some vulnerabilities that get discovered never get reported to CISA, but they allow companies to feed their own risk analysis, risk management or a high-level risk assessment.

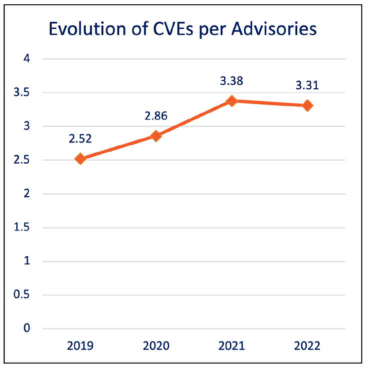
EXECUTIVE SUMMARY

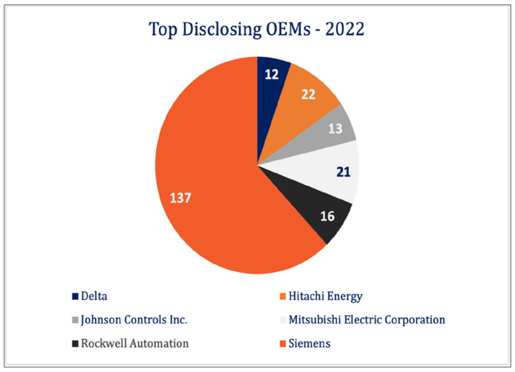
In 2022, ICS-CERT issued 370 cybersecurity advisories available for public consumption on CISA's website (Cybersecurity & Infrastructure Security Agency). Verve analyzed these advisories without any discrimination - no advisory was rejected based on geography, company size, domain of operations, vendor, etc. The only advisories not included in the analysis were those related to medical devices (ICSMA) and those republished or reanalyzed by CISA. So only the advisories starting with ICSA-22-***-** were kept as part of the scope of this analysis. This report summarizes the conclusions, the observed trends, and a perspective on what 2022 might hold.

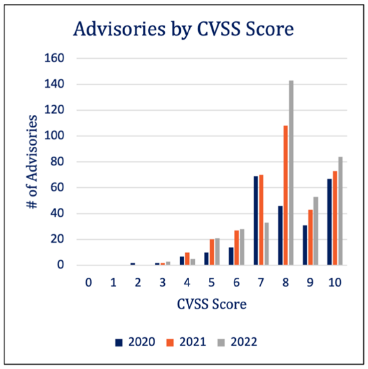
ICS-CERT released 370 ICS-related advisories spanning more than 85 vendors/OEMs, 1,225 CVEs containing references to different products and a matrix of affected versions.

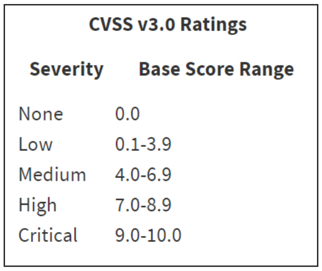
ICS-CERT advisories were basically flat year over year (an increase of ~4.3% over 2021), with the number of CVEs growing by ~2.2%. This is the smallest growth observed by the Verve research team since we started doing this yearly analysis in 2019-20. Previous years all had change above 20 to 40% for both the number of advisories and the number of CVEs.

The OEMs/Companies most affected by the ICS advisories have stayed relatively consistent since 2020, with Mitsubishi Electric consistently part of the top 5 for the last few years and Siemens still being the OEM with the highest number of advisories to its name.









CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Many of the risks created by those vulnerabilities are considered HIGH or CRITICAL by NIST's National Vulnerability Database (NVD), with a significant increase of those scored with a CVSS of 9 and 10/10 (Critical) and those scored as High (~8).

280 advisories out of the 370 had a score of 8 or higher in 2022. Of those advisories, 203 (73%) are exploitable remotely, 262 (94%) have a low attack complexity, and 13 have public exploits available.

With the rise of IIoT, IT systems in OT environments and remote network connectivity, the risk of lateral movement and privilege escalation increase as well. Therefore, it is important for organizations to be mindful of what they have in their environment and the ICS vulnerabilities that apply to them. Organizations should especially look at the vulnerabilities that have known exploits, as it means a threat actor has exploited them in the past.

The following trends are also observed:

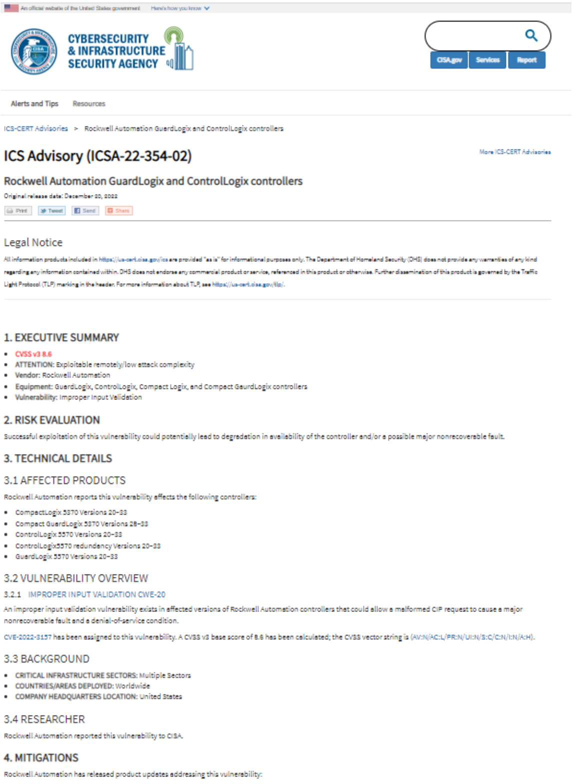
- A good portion of the vulnerabilities could be used to impact the critical manufacturing sector (40%).
- More than half of all the reported vulnerabilities could affect more than one sector (53%).
- There is a decrease in the number of vulnerabilities affecting multiple products compared to 2021 (-4%), but still 129 advisories in 2022 that can affect multiple products (137 in 2021).
- Most of the vulnerabilities have been identified for companies headquartered in 6 specific countries (90%).
    - This includes Germany, which can easily be explained by the fact that Siemens is headquartered there.

In 2022, like in 2021, Siemens had the largest number of advisories. In 2022, 37% of alerts were related to Siemens against 36% in 2021. The high number of advisories doesn't mean that Siemens is less secure than their competitors, but instead that a lot of research and threat hunting has taken place for Siemens products and solutions. This is shown by the fact that 85 advisories out of the 137 (62%) published by CISA on Siemens in 2022 were self-reported – either reported by Siemens itself or by a researcher working for the organization. This shows that Siemens most likely has a mature threat-hunting team and vulnerability management program. If, for most or all these advisories, Siemens was to provide a fix, a patch or a mitigation solution (like they have in most of the advisories published in 2022), they can ensure that their products are part of the most secured out there.

METHODOLOGY AND DATA

To collect data for comparison to the observations published for 2021, the Verve research team applied a similar approach:

- We collected all the ICS CERT advisory results and CVEs.
    - We removed advisories that focused on medical devices (ICSMAs).
- We analyzed the results and reviewed for any discrepancies or gaps in the 2022 period:
    - The nature of the disclosure based on available data.
    - The cause noted in the advisories and the different CVEs they contained.
    - The consistency and exactitude of information contained in the advisories.
- We compared the results with previous years in order to understand trends within the OT market and threat hunting.
- We reviewed the results and aggregated them together into multiple dashboards for final analysis.



ICS-CERT Advisories > Rockwell Automation GuardLogix and ControlLogix controllers

ICS Advisory (ICSA-22-354-02)

Rockwell Automation GuardLogix and ControlLogix controllers

Original release date: December 20, 2022

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1. EXECUTIVE SUMMARY

- CVSS v3 8.6
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Rockwell Automation
- **Equipment:** GuardLogix, ControlLogix, Compact Logix, and Compact GeurdLogix controllers
- **Vulnerability:** Improper Input Validation

2. RISK EVALUATION

Successful exploitation of this vulnerability could potentially lead to degradation in availability of the controller and/or a possible major nonrecoverable fault.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Rockwell Automation reports this vulnerability affects the following controllers:

- CompactLogix 5370 Versions 20–33
- Compact GuardLogix 5370 Versions 28–33
- ControlLogix 5570 Versions 20–33
- ControlLogix5570 redundancy Versions 20–33
- GuardLogix 5570 Versions 20–33

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER INPUT VALIDATION CWE-20

An improper input validation vulnerability exists in affected versions of Rockwell Automation controllers that could allow a malformed CIP request to cause a major nonrecoverable fault and a denial-of-service condition.

CVE-2022-3157 has been assigned to this vulnerability. A CVSS v3 base score of 8.6 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).

3.3 BACKGROUND

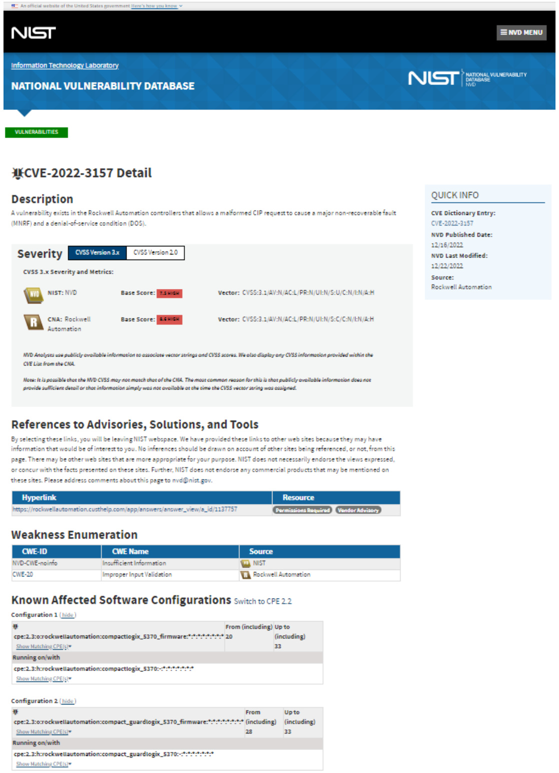
- **CRITICAL INFRASTRUCTURE SECTORS:** Multiple Sectors
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

3.4 RESEARCHER

Rockwell Automation reported this vulnerability to CISA.

4. MITIGATIONS

Rockwell Automation has released product updates addressing this vulnerability:


An official website of the United States government Here's how you know
NIST
NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES
CVSS Version 3.x
CVSS Version 2.0
Switch to CPE 2.2
hide
Show Matching CPE(s)

CVE-2022-3157 Detail

Description

A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS).

QUICK INFO

CVE Dictionary Entry: CVE-2022-3157
NVD Published Date: 12/16/2022
NVD Last Modified: 12/22/2022
Source: Rockwell Automation

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 7.5 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CNA: Rockwell Automation	**Base Score:** 8.6 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	Permissions Required Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-noinfo	Insufficient Information	NIST
CWE-20	Improper Input Validation	Rockwell Automation

Known Affected Software Configurations

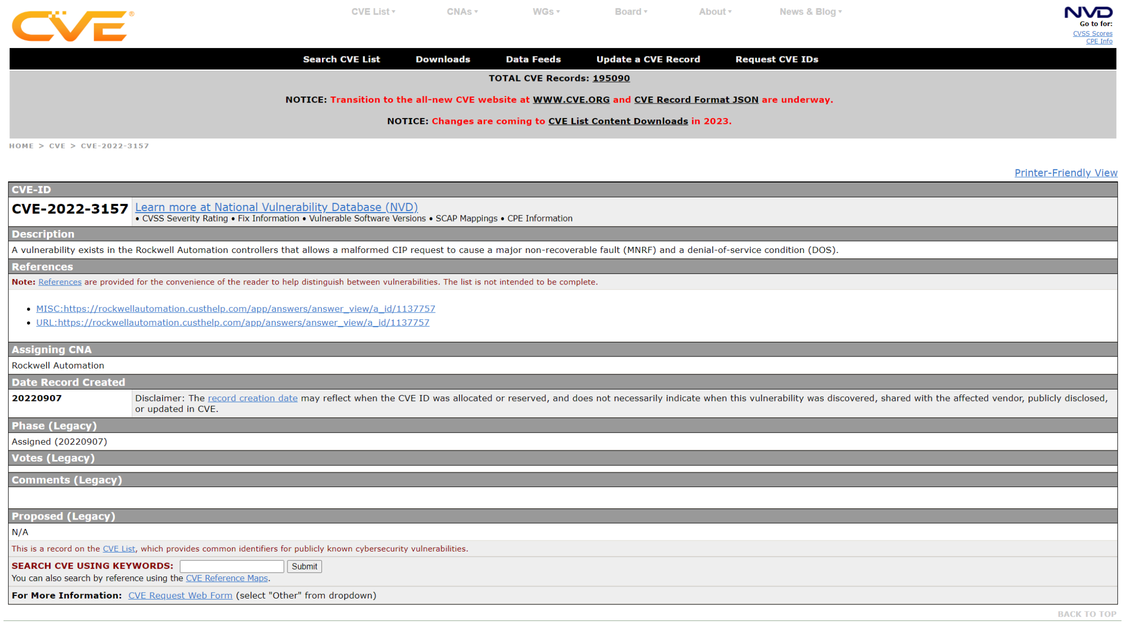
Configuration 1

	From (including)	Up to (including)
cpe:2.3:o:rockwellautomation:compactlogix_5370_firmware:*:*:*:*:*:*:*:*	20	33
Running on/with		
cpe:2.3:h:rockwellautomation:compactlogix_5370:-:*:*:*:*:*:*:*		

Configuration 2

	From (including)	Up to (including)
cpe:2.3:o:rockwellautomation:compact_guardlogix_5370_firmware:*:*:*:*:*:*:*:*	28	33
Running on/with		
cpe:2.3:h:rockwellautomation:compact_guardlogix_5370:-:*:*:*:*:*:*:*		

We analyzed each ICS-CERT advisory for severity, exploit vectors, link to product names and software versions, what the relevant risk entailed, etc. They were recorded, visited, and their information archived.



TOTAL CVE Records: 195090

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Changes are coming to CVE List Content Downloads in 2023.

HOME > CVE > CVE-2022-3157

Printer-Friendly View

CVE-ID

CVE-2022-3157 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS).

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757
- URL:https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757

Assigning CNA

Rockwell Automation

Date Record Created

20220907 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20220907)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

BACK TO TOP

We checked to see if CVEs were missing/reserved, validated scores to determine if they were marked correctly and did the CPE strings reflect initial expectations (e.g., did the vendor's name match, or was the product's name correct?).

The information was cross-referenced with data from previous years to identify tendencies and changes in the ICS market.

370 ICS Advisories

4.3% increase

1225 CVEs

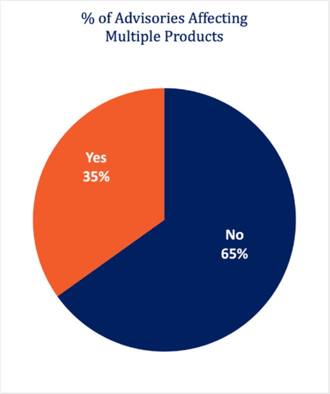
2.5% increase

Average 7.93 CVSS

0.3% increase

ANALYSIS & FINDINGS

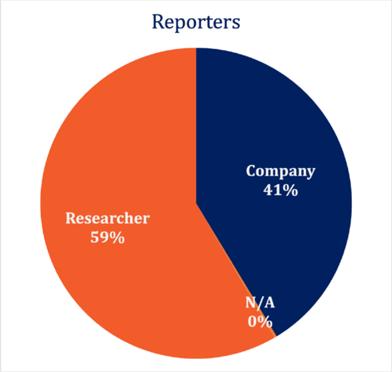
Analysis of ICS vulnerabilities based on CISA advisories



Verve analyzed the ICS-CERT alerts for the past several years. This provides a comprehensive view of all the publicly released vulnerability information. The data shows a stabilization in the number of advisories published each year. While previous years used to be drastically more important than the one before, the year 2022 has only a minimal elevation.

At a high level, Verve found a minimal increase in the total number of advisories in 2022 vs. 2021 and the number of CVEs. With an increase of 4.3% in the number of advisories published in 2022 compared to 2021, the difference is far from the 30% increase that was observed between 2021 and 2020.

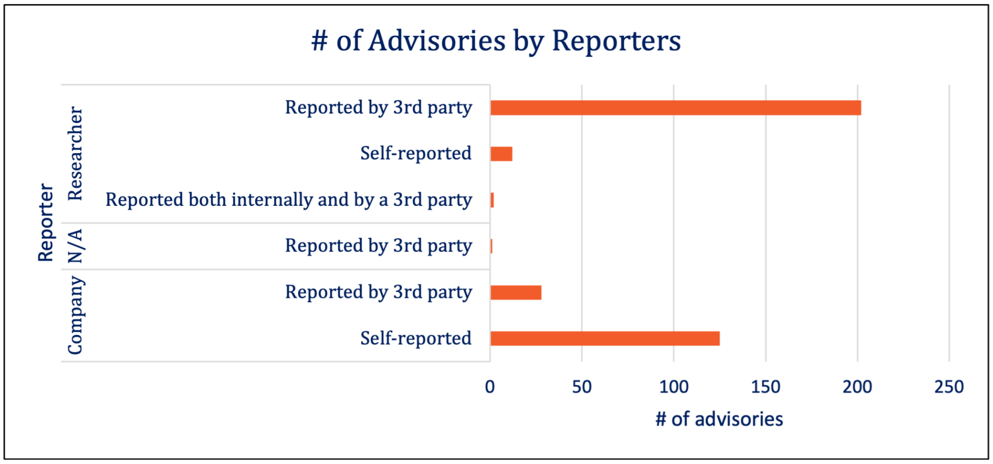
OT/ICS being what it is, it is impossible to think that all these vulnerabilities will be patched by critical infrastructure and operational companies in a timely matter, if at all. ICS organizations need to ensure they put controls or compensating controls in place to secure their environment, but many don't know where to start. Looking at the advisories that concern one's network/organization could be a good start to understanding where some of the vulnerabilities and risks may be.



Of the ~390 original ICS-CERT advisories, medical devices (ICSMA) were excluded. Of the remaining 370 advisories, the average CVSS score was 7.93 (High). The average number of vulnerabilities (CVEs) per advisory was also significantly higher than one.

In addition to the above summary statistics:

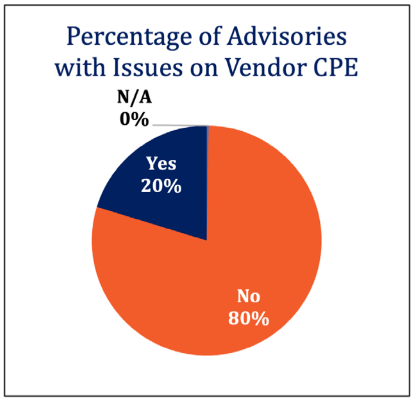
- 65% were both exploitable remotely with low skill or with low attack complexity, compared to 60% in 2021



- 129 affected multiple products (35%) compared to 137 (39%) in 2021, and 351 affected multiple versions (95%)
- Average of 3.31 CVEs per advisory, with one of the advisories having more than 80 CVEs (ICSA-22-349-21 with 83 CVEs)

Observations	2019	2020	2021	2022
# of applicable advisories	192	248	354	370
# of CVEs	484	710	1198	1225
~ average CVSS score from advisory data	7.85	8.01	7.91	7.93

Discovery & Reporting



- 216 ICS-advisories were reported by researcher(s) (~59%), 153 by company (~41%) and compared to previous years (e.g. 2020), none of them were reported by a government entity. One of the advisories was unmentioned/unknown (~0%).
- 137 advisories were self/company reported, which means they were either reported by a researcher working for the company or the company itself reported the advisory to CISA. 2 were reported together by both a researcher from the company and an external/3rd party one.
- This is almost the same amount as last year, where 140 advisories were self-reported.

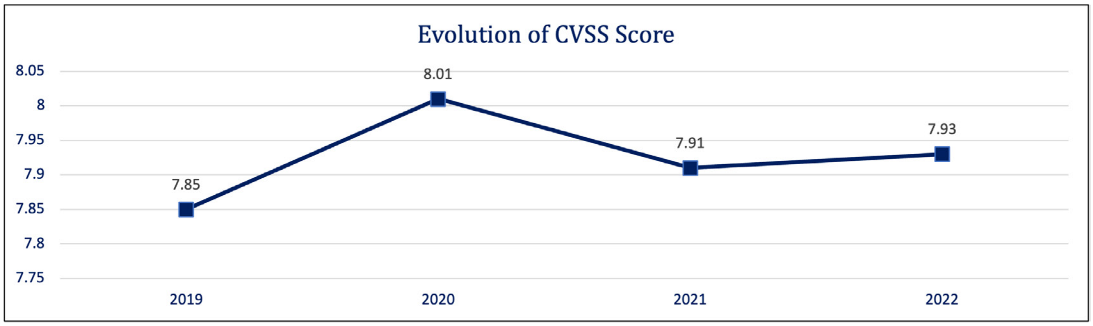
- The list of researchers contains independent researchers and members of research groups or companies that are third-party to the one targeted by the advisories.
- Around 20% had issues when comparing advisory details.
- Those issues ranged from reserved CVEs (CVE ID Not Found) to the absence of CPE in the CVE, Third-party CPE in the CVE instead of the vendor ones, and even CVEs undergoing analysis or reanalysis.
- However, not all of those issues will be permanent on CISA's website. As explained by one of Verve's researchers in a monthly advisory report, many advisories present problems as they have not yet been completed – The analysis of the vulnerability may be ongoing, CISA may be waiting for additional information from the company or researcher that reported the vulnerability, etc.

While these numbers are large and growing, this analysis excludes two types of additional vulnerabilities: 1) those that vendors do not release publicly but share privately with their clients only, and 2) those that are still hidden in these "insecure by design" systems.

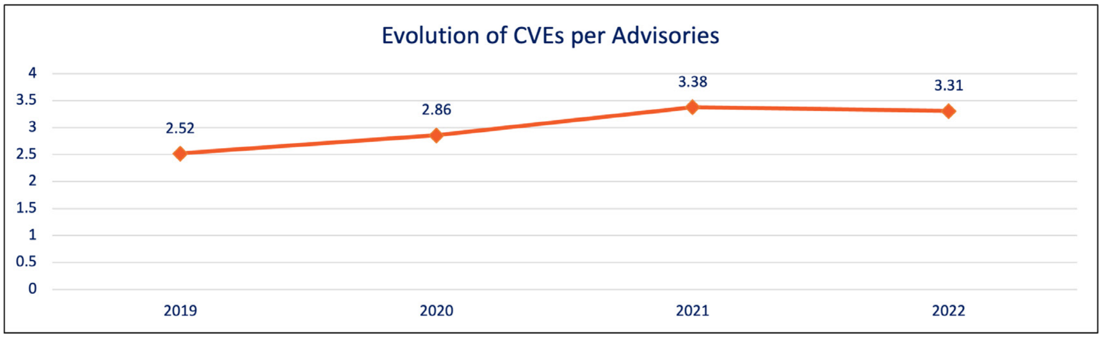
These are some of the reasons why it is so challenging for organizations to manage ICS vulnerabilities and risks in their environment. Many vendors develop devices without any security in mind and never release information on their potential vulnerabilities or ways to fix/mitigate them. It often ends up being the responsibility of asset owners to know the environment, the assets on the network and the industrial process to find ways to secure the network – with many organizations lacking updated documentation. Usually, many ICS vulnerabilities and potential threats end up falling through the cracks.

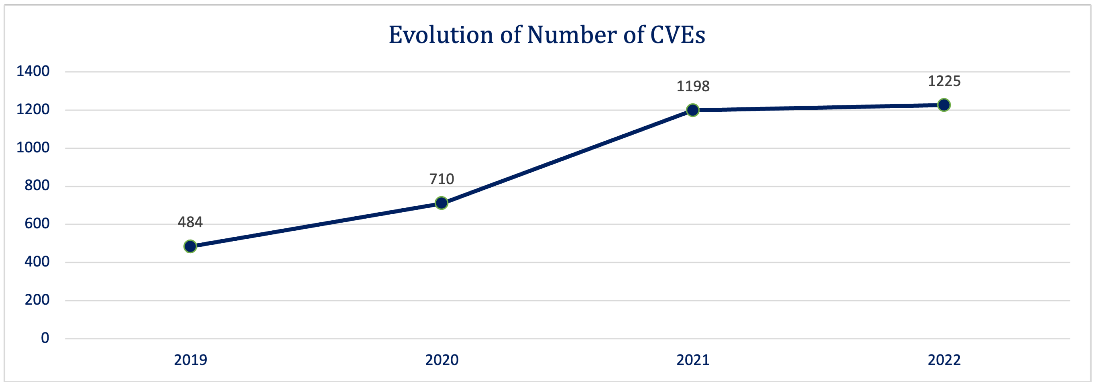
CVSS Ratings

The average CVSS scores have remained consistent over the years even as the number of CVEs increased drastically:



- On average, there were 3.31 CVEs per CVSS in 2022, which is almost the same as in 2021.
  - This is less than in the previous year, and the first time the average number of CVEs per advisory has decreased in the last few years.





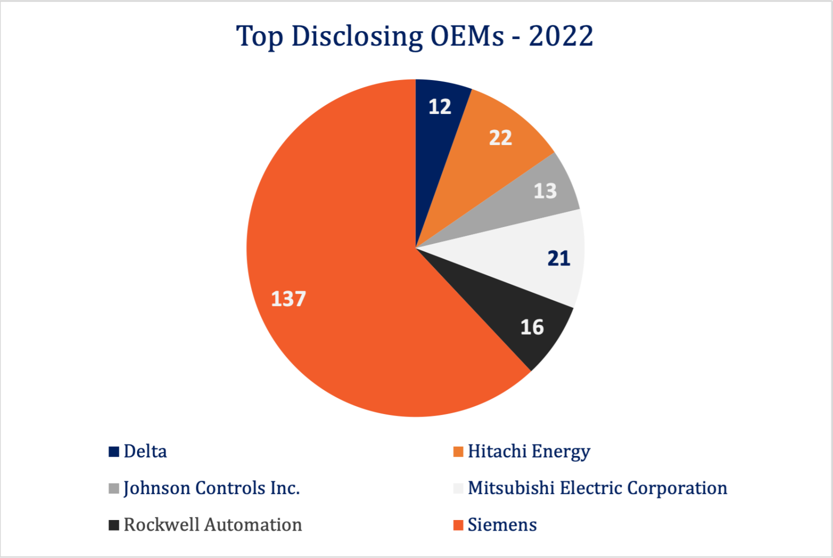
- While the number of CVEs per advisory has been relatively consistent and even decreased in 2022 compared to 2021, the overall number of CVEs increased by 27 between 2021 and 2022, as shown in the following graph.
    - This is a minimal increase considering that the number of advisories grew by 16. If we compare the number of additional advisories with the additional CVEs, the number of CVEs per advisory would still be higher than one (27 / 16 = 1.69 CVEs per CVSS).
- We took a random sample of ICS advisories to establish the discrepancy between the CVSS score and the suggested scores from the CVE(s) they contained. We saw some minor discrepancies but nothing major. Of course, some advisories still have significant gaps between their scores and those attributed to the CVEs they contain. Asset owners should therefore stay vigilant.
    - ICSA-22-132-04 had a CVSS score of 9.8 and 7 CVEs, with scores suggested at 9.8 (For 2 CVEs), 7.5 & 7.8.
    - ICSA-22-298-07 had a CVSS score of 9.8 and a total of 10 CVEs, with scores ranging from 7.5 to 9.8. The average score of the CVEs was 9.07.
    - ICSA-22-069-01 had a CVSS score of 6.7 and one CVE score of 6.5. There is a slight discrepancy here, but the NVD considers both scores Medium.

Vendor Disclosures

The vendors with the most disclosures have stayed relatively consistent over the years, but we can observe a few changes when we compare the top OEMs from 2022 with the ones from 2021.

In 2022, the top three vendors were:

- Siemens with 137 advisories, which represent 37% of all the advisories that were published in 2022.
- Hitachi Energy with 22 advisories (~6%), which during the previous year was not part of the 5.
- Mitsubishi Electric with 21 advisories (~6%), which represents 4 more advisories than the previous year.



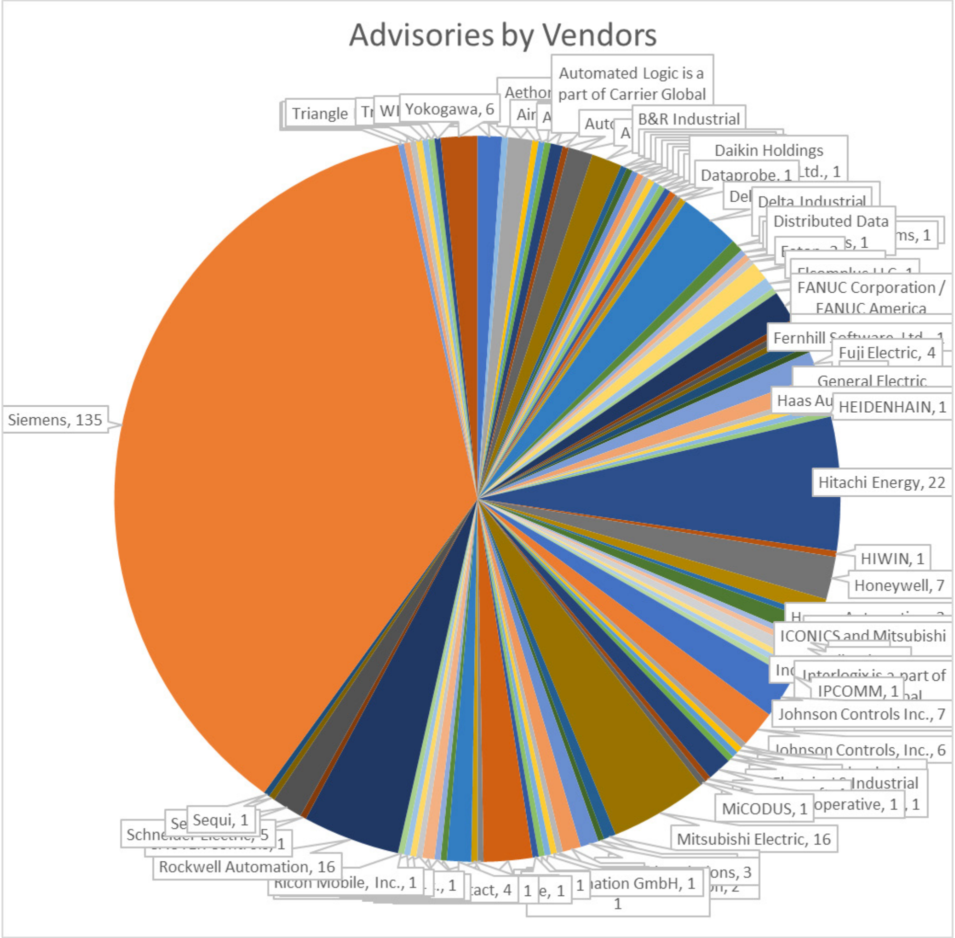
This doesn't come as a surprise as Siemens was also the top disclosing OEM in both 2020 and 2021, where they reported 73 and 129 advisories to CISA.

By looking at the entire data sample, it is possible to observe the following:

- Advantech, who notably was part of the top 5 OEMs with the most advisories to its name in the last two years (2020 & 2021), only had 4 advisories to its name in 2022.
- Johnson Controls had 21 advisories to its name in 2021, having reported many advisories for some of its subsidiaries – In 2022, however, it only reported 13 advisories, with very few regarding their subsidiaries.
- In 2022, CISA reported advisories and vulnerabilities for 86 vendors.

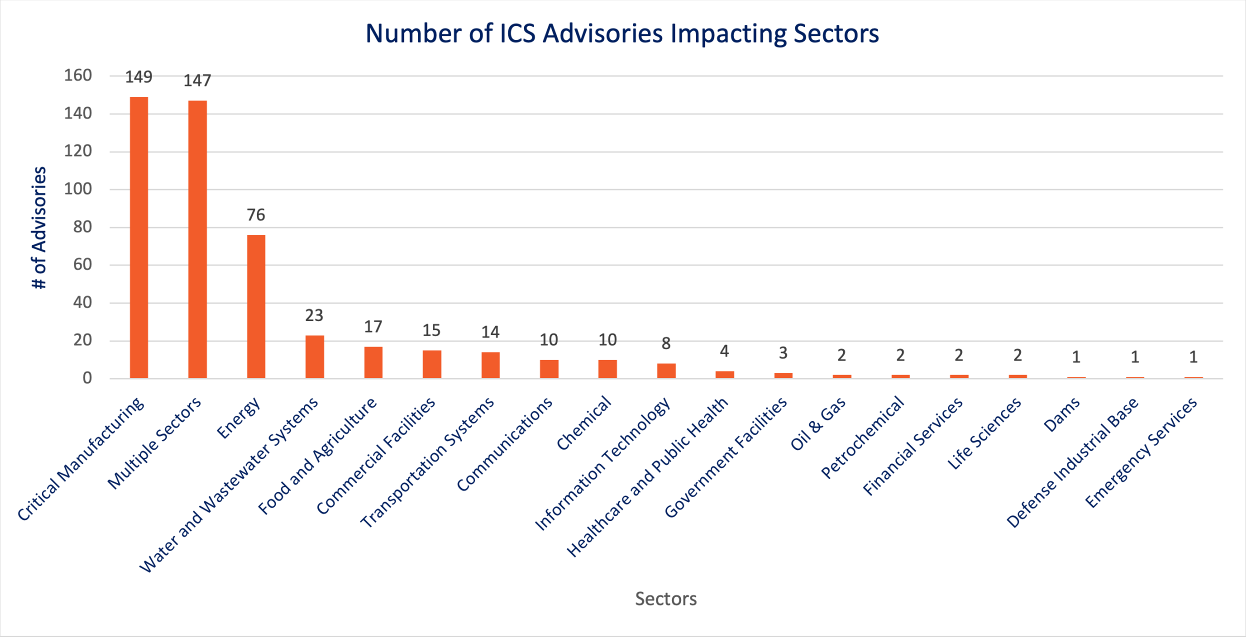
In addition, from a data perspective, this chart has multiple caveats that a reader needs to be aware of:

- Many vendors are not reporting ICS vulnerabilities or sharing the vulnerabilities with affected customers. These vulnerabilities still exist but are not on the list of advisories.
- Many products impacted by the ICS vulnerabilities are end-of-life and will not receive a patch or other corrective measure. Asset owners need to add compensating controls around those products.
- Many advisories impact 3rd party software and could impact vendors that are not listed in the advisory itself.
- Of those vendors, many reported vulnerabilities to CISA, but for the most part, external researchers had to send the vulnerability to CISA. The fact that a researcher reported a vulnerability to CISA does not mean the organization to which it is subject did not previously know about it but decided to keep it in the dark/secret.



Many ICS vulnerabilities impact organizations whose business is in different industry verticals. This can be observed in the chart below where those observations can be made:

- 147 advisories impact “Multiple Sectors” but does not specify which Industry they touch
- 175 advisories only impacted one sector (e.g. only Energy)



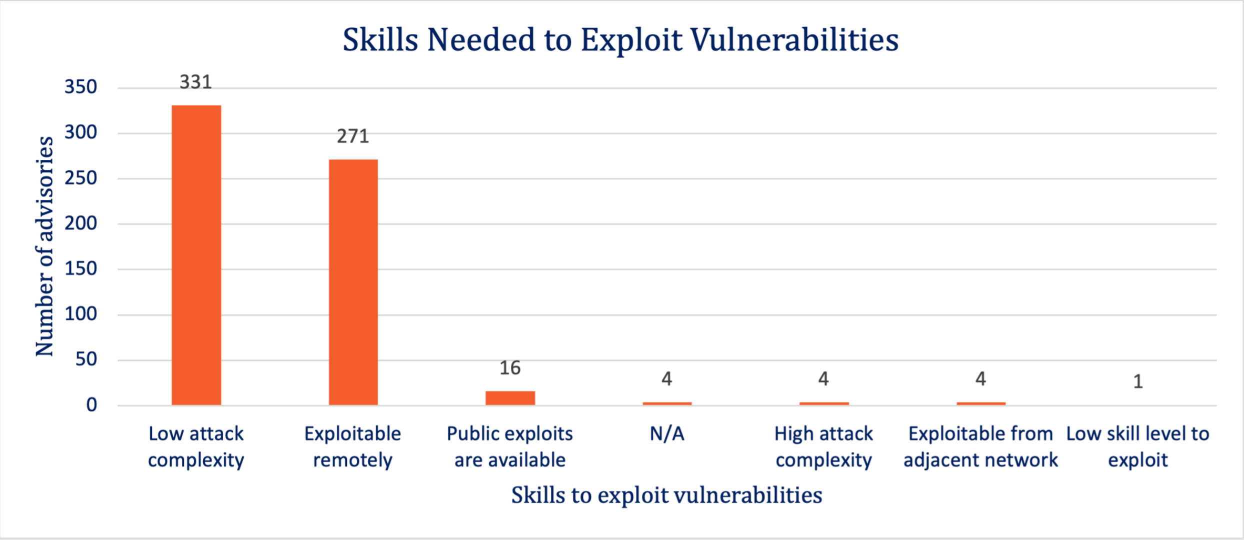
- The industries with the most ICS vulnerabilities found were Critical Manufacturing (40%), Energy (21%), and Water & Wastewater Systems (6%). Those were also the most affected by the advisories in 2021.
    - Those three industries have been prime targets for threat actors for the last few years. Those sectors are all part of the critical infrastructure that governments need to ensure stays secure – the impact of a major outage could have critical ramifications on safety and the population’s wellness.
- Other industries significantly targeted by the advisories/vulnerabilities found were Food & Agriculture (5%), Commercial Facilities (4%), Transportation (4%), Communications (3%) and Chemical (3%).

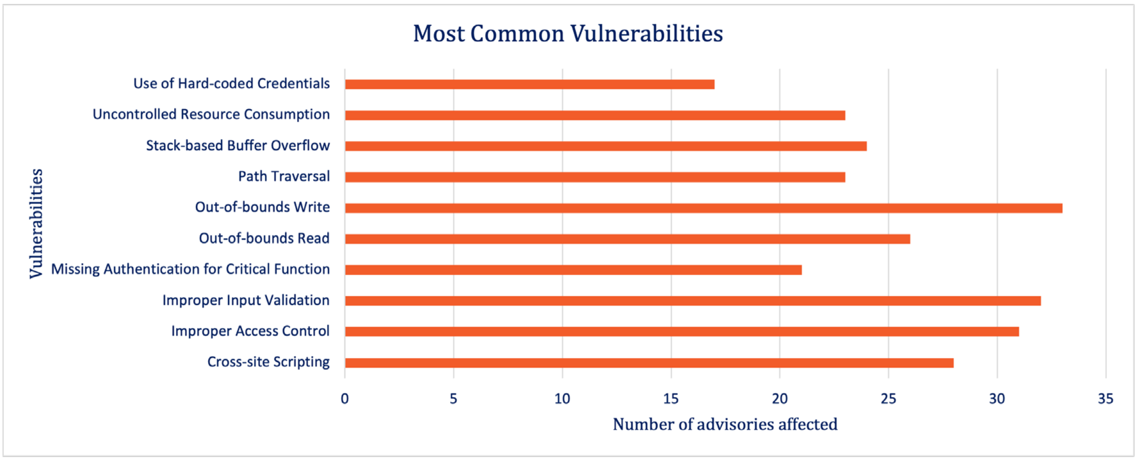
OT is clearly in the crosshairs of cyber attackers, and manufacturing is at the center of all the OT/ICS cyber warfare.

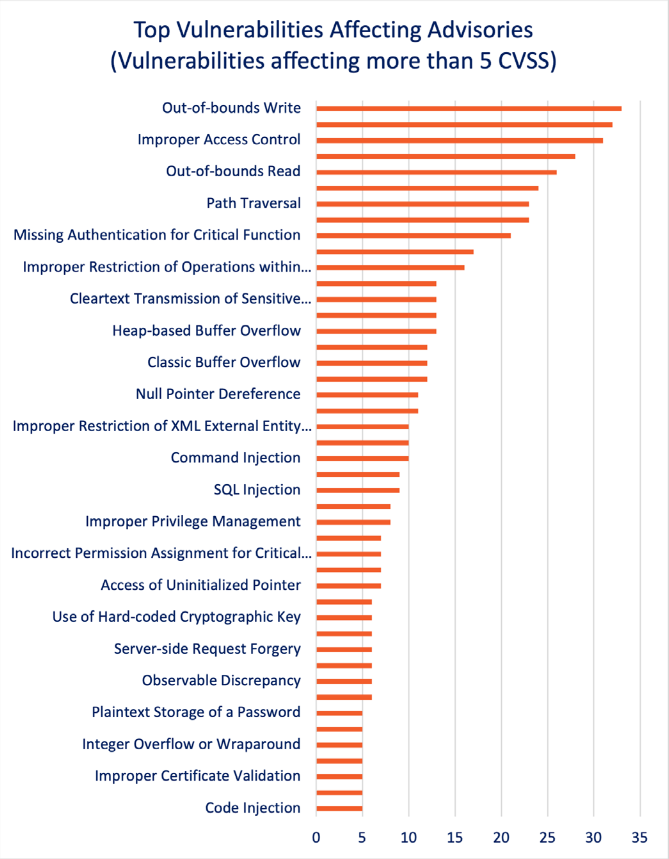
Top Vectors & Issues

When we looked at the previous year (2021), we saw that 67% of the advisories could be exploited remotely, and 75% had a low attack complexity. For 2022, those numbers were significantly higher - If an attacker gains access, most ICS vulnerabilities have a low attack complexity (~90%) or are exploitable remotely (73%).

The details for 2022 are presented below:





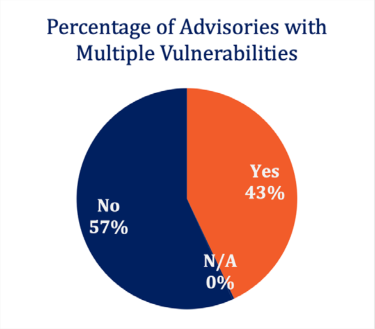


198 unique vulnerabilities/issue values were found. After doing sorting and counting, the top 5 vulnerabilities, as well as their frequency within CVSS are as follows:

- Out-of-bounds Write: ~9%
- Improper Input Validation: ~9%
- Improper Access Control: ~8%
- Cross-site Scripting: ~8%
- Out-of-bounds Read: ~7%

In previous years, there may have been lesser occurrence counts partially due to the overall numbers of CVEs being significantly lower (488 more CVEs in 2021 compared to 2020), but between 2022 and 2021, the number of overall CVEs has only raised by 27.

However, there are similarities with 2021 when we look at the most common vulnerabilities that were reported by CISA in the ICS advisories. Out-of-bounds Read, Out-of-bounds Write & Improper Input Validation were all part of the top 5 unique vulnerabilities for both 2022 and 2021, for example.



Of the 198 unique ICS vulnerabilities that were found, 160 only affected between 1 and 5 advisories. This means that only 19% of the vulnerabilities identified impact more than five advisories. By adding all the vulnerabilities that impact many vendors, we got a total of 785 vulnerabilities for 370 advisories (1 advisory had no specified vulnerabilities). In 2021, the total was 795 (+25 compared to 2022) for 354 advisories, therefore explaining why the average number of CVEs per advisory was higher in 2021 than in 2022.

With this high number of ICS vulnerabilities, more than twice the number of advisories published in 2022, it is expected that a significant proportion of the advisories had more than one vulnerability associated with them. According to the data the Verve research team collected, 43% of the advisories, so around 159 advisories (of those, 2 advisories had "Multiple" listed as "Type of vulnerability", but those vulnerabilities weren't specified in the advisory), had more than one vulnerability associated to it.

This is 1% less than the previous year but is still a significant number that asset owners and OT cybersecurity specialists should pay attention to. In the end, many of those advisories and vulnerabilities don't have an all-inclusive fix or an easy solution for mitigation. However, asset owners should focus on specific ones rather than tackling the complete list available. Understanding the organization's risks and prioritization is critical.

Known Exploited ICS Vulnerabilities

Over the past couple of years, CISA has produced a database titled the KEV "Known Exploited Vulnerability" Catalog. The KEV lists all vulnerabilities where a known exploit exists. This catalog is incredibly helpful for focusing the security team's time on those vulnerabilities that are most likely to pose an active risk. Most of the ICS advisories do not have a known vulnerability when the advisory is released, although the percentage is growing. In 2022, roughly 5% of the 370 public advisories had a known public exploit. This compares to only 2/340 in 2021.

This doesn't mean that no exploit could exist for the other 354 advisories released in 2022 – as you can see from the difficulty score, most are a low degree of difficulty to exploit. It is just that know known exploit has been observed "in the wild". Therefore, asset owners should still stay vigilant and consider the exploitability of the different vulnerabilities that potentially affect them and their environment. Furthermore, as mentioned above, there are a large number of vulnerabilities tied to the IT-type devices found in OT than require us to be vigilant against known exploits.

As we think about prioritizing remediation, focusing on those with Known Exploits is an initial starting point to focus the efforts of the team.

Importantly, as referenced earlier, the greatest amount of vulnerabilities in most OT environments, especially those with Known Exploits, will not be the advisories that emerge from vendors on their firmware or applications, but instead will be all of the OS-based devices and their Windows patches and application patches for non-ICS software. These will outweigh the critical vulnerabilities from ICS-advisories by 10:1 or more in most cases.

Prioritized vulnerability management in OT, must take into account those risks as a primary threat vector.

EXAMPLE PRIORITY ADVISORIES

During the year 2022, many advisories had to be considered as priorities by organizations regarding remediation. Those advisories either affected them directly or had public exploits available and could be considered as a serious threat to the organization's environment. If the investment required to mitigate an advisory/vulnerability cost less than the potential cost of an incident related to the materialization of that threat, a cyber-mature organization probably would have paid the money to reduce its risk. But in most cases, OT organizations don't necessarily have an effective risk, vulnerability, and patch management program. Therefore, they must decide where to spend their limited budget and time to mitigate the most critical vulnerabilities they can find.

To help organizations pinpoint some of those vulnerabilities, we identified three critical advisories that stand out from the crowd and explained why we consider them noticeable:

ICSA-22-349-21			
CVSS Score	**9.8**	**Skills (CSV)**	● *Exploitable remotely* ● *Low attack complexity* ● *Public exploits are available*
Number of CVEs	**83**		

Vendor	*Siemens*	Types of vulnerabilities	- *Observable Timing Discrepancy* - *Race Condition* - *Improper Restriction of Operations within the Bounds of a Memory Buffer* - *Improper Input Validation* - *NULL Pointer Dereference* - *Use After Free* - *Cryptographic Issues* - *Comparison of Incompatible Types* - *Resource Management Errors* - *Incorrect Calculation* - *Exposure of Sensitive Information to an Unauthorized Actor* - *Permissions, Privileges, and Access Controls* - *Out-of-bounds Write* - *Improper Authentication* - *Integer Overflow or Wraparound* - *Observable Discrepancy* - *Out-of-bounds Read* - *Missing Release of Memory after Effective Lifetime* - *Uncontrolled Resource Consumption* - *Untrusted Search Path* - *Incorrect Permission Assignment for Critical Resource* - *Incorrect Authorization* - *Improper Certificate Validation* - *Improper Encoding or Escaping of Output* - *Inappropriate Encoding for Output Context* - *Path Traversal*
Headquarter	*Germany*		
Product(s)	*SCALANCE X-200RNA switch devices before V3.2.7*		
Sectors affected	*Multiple Sectors*		
Description			
This advisory has the largest amount of CVEs in all the advisories published in 2022. It's vital for organizations using this product to look carefully at all the different elements of this advisory and to understand where they are vulnerable. *This advisory also has public exploits available, which means that at least one of the vulnerabilities listed in this advisory has been exploited in the past and that it is common knowledge (which means that threat actors also know that one of those vulnerabilities at least is exploitable).*			
Mitigation			

To mitigate these vulnerabilities, Siemens recommends updating the switch devices to version 3.2.7 (or later). However, suppose this can't be done by an organization (For example, it would require a reboot of the systems/outage of the operational process, etc.). In that case, they need to ensure that they put compensating controls around these devices.

CISA proposes the following solutions:

- *Restrict access to the affected systems, especially ports 22/TCP and 443/TCP, to only trusted IP addresses.*
- *Deactivate the webserver if not required, and if the product supports deactivation*

ICSA-22-223-02			
CVSS Score	7.6	**Skills (CSV)**	● *Exploitable remotely* ● *Low attack complexity*
Number of CVEs	2		
Vendor	*Siemens*	**Types of vulnerabilities**	● *Command Injection* ● *Infinite Loop*
Headquarter	*Germany*		
Product(s)	*Teamcenter*		
Sectors affected	*Multiple Sectors*		
Description			
This advisory should have been scored higher based on the fact that it could potentially and likely lead to Denial-of-Service if the vulnerability was to get exploited and that there is no specific mitigation method that can be taken to reduce the risk appropriately. The vulnerability also impacts a lot of the different versions of Teamcenter. The CVEs associated with it are also scored High or critical (7.5 and 9.8).			
Mitigation			
There is no patch proposed by Siemens to mitigate this vulnerability. Siemens has identified work-arounds and mitigations /compensating controls to reduce the risks created by the vulnerability, such as hardening the application, limiting access to it and ensuring Teamcenter is used behind a firewall.			

A lot of other vulnerabilities could be listed above. Many advisories published in 2022 represent a real risk to numerous operational organizations. In the end, organizations must make sure they filter on what matters to them, their environment and critical systems and eliminate as much "noise" as possible in order to focus on what matters.

One important note is that many ICS vulnerabilities are not found easily within the National Vulnerability Database. In many cases, such as the one shown below, the ICS advisory comes out relating to an ICS vendor (in this case Rockwell) but the underlying CVEs are tied to the product manufacturer, in this case CISCO, rather than the OEM'd version of that device. Organizations need to be cognizant of this risk of missing a true picture of the vulnerabilities and ensure that when evaluating risk, these anomalies in the data are captured.

ICSA-22-300-03			
CVSS Score	8.8	**Skills (CSV)**	- *Exploitable remotely* - *Low attack complexity*
Number of CVEs	9		
Vendor	*Rockwell Automation*	**Types of vulnerabilities**	- *Incorrect Authorization* - *Improper Input Validation* - *Improper Check for Unusual or Exceptional Conditions* - *Interpretation Conflict* - *OS Command Injection* - *Improper Verification of Cryptographic Signature* - *Path Traversal*
Headquarter	*United States*		
Product(s)	*Stratix Devices*		
Sectors affected	*Multiple Sectors*		

Description

CISA should review this advisory as all the CPEs in the CVEs point back to Cisco and their iOS and even reference their website. However, the advisory is still mentioned as being for Rockwell Automation. Even if Rockwell uses Cisco's OS in some of their assets, all the CVEs are about Cisco, and none mentions Rockwell or Allen-Bradley.

Also, many other devices other than those mentioned in the advisory (Stratix 5800 switches and Stratix 5400/5410 switches) are affected by the vulnerabilities mentioned in the CVEs – e.g., Allen-Bradley Stratix 5900 Services Routers or some Allen-Bradley Stratix 8300 Industrial Managed Ethernet Switches for example. So, the list of affected devices doesn't seem accurate.

The CVEs associated with it are scored between 4.3 and 8.8 {4.3, 6.5, 6.8, 7.2(x2), 7.7, 8.6, 8.8(x2)}, with most of them being inconsistent with the CVSS score – The discrepancy with the scores is pretty significant.

Mitigation

Rockwell Automation encourages users to combine multiple updates with their own Security Best Practices and update the Stratix 5800 and 5400/5410 switches to a later version.

Cisco offers no mitigation solutions in the advisory. But if asset owners go into the CVEs, there are some links to Cisco's website where they offer their own Security advisories, with potential workarounds and remediation solutions.

For more information, Cisco offers a "Cisco Software Checker" online that could allow asset owners to check for Security Advisories that affect specific releases of some of Cisco's software.

REMEDIATION

The above summary can be overwhelming for an asset owner or site engineer. One question that arises the most regarding ICS advisories is: Where do I start with all of this?

As mentioned previously in this report, the ICS-advisories and CISA alerts on ICS products are really only the tip of the iceberg when it comes to risks and vulnerabilities in OT. The vast majority of the vulnerabilities found in our assessments of OT environments are on the Windows/Unix/Linux assets and their OS and non-ICS software, rather than the pure ICS vulnerabilities. Furthermore, because so few of the ICS-advisory CVE's have known exploits, the greatest risk is certainly to these Windows assets. However, the way to assess and remediate risks to those OS versions and applications in OT is not the same as IT. Normally, vulnerability scanners cannot operate safely in these environments, and remediation can be time consuming or costly trying to coordinate with local sites and vendors. As we consider how to prioritize vulnerabilities, these need to be top of the list.

The answer to OT vulnerability management requires considering a range of questions – What is your organization's risk appetite, what is the budget, what is the impact of an incident, which assets are critical in your environment, etc. There have been more and more advisories published by CISA each year, and the number of ICS vulnerabilities being discovered won't decrease either. With more advisories and vulnerability information being made available to the public, organizations have more data than ever to use in their risk management program -- and hackers also have more information to work with. The game for organizations then becomes:

To assess their risk quickly and efficiently:

- Have an automated vulnerability assessment approach that gathers detailed vulnerability information, and known exploits across the Windows/Unix/Linux OS devices as well as the ICS advisory vulnerabilities. This requires a very deep and accurate asset view and OT-specific vulnerability identification approach that is "OT-safe"
- 360-degree risk assessment. Because many vulnerabilities do not have a patch or cannot be patched immediately, it is critical that the organization look beyond just patching and updating to a broader set of mitigation.
- Establish an organization that can "Think Global, and Act Local" to remediate these vulnerabilities. This means gathering these risks into an enterprise central reporting system so a small, focused team can prioritize across the risks. However, for remediation, "local" control to ensure that these actions are done with the expertise of those that know the process.
- Likely pursuing a range of mitigating measures rather than just patching including the recommendations that CISA offers.

CISA offers numerous recommendations to remediate the ICS vulnerabilities they report in their advisories. Those include:

- Patching the vulnerability
- Updating the firmware or software to a more recent version that doesn't have the vulnerability.
- Minimize network exposure for all control system devices and systems, and ensure that they are not accessible from the internet
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also, recognize VPN is only as secure as its connected devices
- Manage the security of the "upstream" devices above the ICS embedded controllers, etc. This includes HMIs, servers, networking devices, etc. Hardening these systems includes patching, hardening configuration settings, etc.
- Applying application whitelisting and updated AV tools on HMIs, servers, and other management devices.

Please see the link regarding our "Technology Enabled Vulnerability Assessment".

Of course, no ICS asset owner can patch all those vulnerabilities. Most ICS systems have a small threshold for risks related to patching (downtime, critical systems that cannot be rebooted, old systems that cannot be patched for performance reasons, etc.). But by using the information compiled by CISA, asset owners can monitor the potential risks for their organizations based on the vendors they have in their environment, apply cybersecurity controls if possible or compensating controls, and even integrate that information into their vulnerability management and threat hunting.

Those methods are particular to the advisories they are part of. This doesn't mean that an organization can simply follow them by the book and patch/update their assets/ systems/software as it pleases them.

As mentioned in last year's report, we at Verve proposed five key remediation actions to start:

- First, companies should ensure they have a comprehensive asset inventory, including embedded devices, software, firmware, etc. This should be combined with data from vendors and sources such as CISA.
- Second, organizations should assess the impact of the relevant advisories for their organizations and develop a remediation strategy to mitigate those vulnerabilities.
- Third, ensure OT assets and systems are protected from inappropriate actions as well as malicious application operation. Because of the natural "insecure by design" nature of these devices and systems, operators need to assume that each device has unknown vulnerabilities and ensure protection of assets.
- Fourth, monitor the network for a potential exploit of one of the vulnerabilities.
- Fifth, ensure you're ready to react to a potential incident linked to one of the advisories/vulnerabilities affecting the environment.

Another point to consider is the work that is being done with OEMs. A lot of critical infrastructure organizations rely heavily on OEMs to maintain some of their assets and allow those vendors to connect remotely to their network without necessarily restricting the window in which they should/can access and sometimes by using software that is known to be potentially risky such as Teamviewer (For example), which can already be rather precarious for the OT organizations. On top of that, those OEMs, when they connect remotely to the assets – or even when they come directly on-site to do some maintenance – don't necessarily try to mitigate some of those vulnerabilities published in CISA's ICS advisories. They mostly ensure that the operational process is working correctly and that the assets are working as they're supposed to be. This is why, on top of those five key remediation actions listed in the previous report, Verve's research team recommends that asset owners and companies review their SLAs with those vendors and ensure that mitigating potentially critical vulnerabilities is part of the contract with those vendors. This should also be an essential criterion when looking at potential new partners/vendors.

To conclude, what will happen with 2023 remains to be seen, but one thing is sure: If we look at the numbers for 2022 and tendencies observed over the last few years, we can easily assume that the number of ICS advisories reported each month, and each year won't go down. Therefore, organizations need a solid core of people, process, and technology regarding asset, vulnerability, and risk management.

VERVE

A ROCKWELL AUTOMATION COMPANY

verveindustrial.com

info@verveindustrial.com

888-756-3251