VERVE
A ROCKWELL AUTOMATION COMPANY

2021-22
ICS ADVISORY REPORT

Verve Industrial and our objective

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 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.

Introduction

2021 was a difficult year for everyone – political tensions were high in the East, the COVID-19 pandemic was in full swing, and with everyone homebound, the number of attacks increased considerably on both OT and traditional IT sectors.

During that tumultuous year, and with time on their hands, threat actors pounced on the opportunity to make money as they realized a high number of laptops were deployed outside regular working environments (with people using work laptops for personal activities at home), lower security in a lot of sites, and financial difficulties for a lot of employees (which leads to internal threats).

To provide more information on the threat landscape for ICS, Verve's research team looked at updating the analytical comparison completed last year regarding the trend of ICS advisories and CVEs. To get a better view of growing risks and vulnerabilities, Verve analyzed publicly available data points and reviewed our own vulnerability analysis data from the past couple of years.

In our research, we:

- Examined the 354 ICS-CERT advisories for 2021 and extracted the key insights
- Compared all 2021 advisories with the 248 from the previous year (2020)
- Assessed the potential implications of those advisories
- Developed a list of recommendations for ICS staff based on our observations

Vulnerabilities do not provide a comprehensive threat landscape but allow companies to feed their own risk analysis or an initial risk assessment.

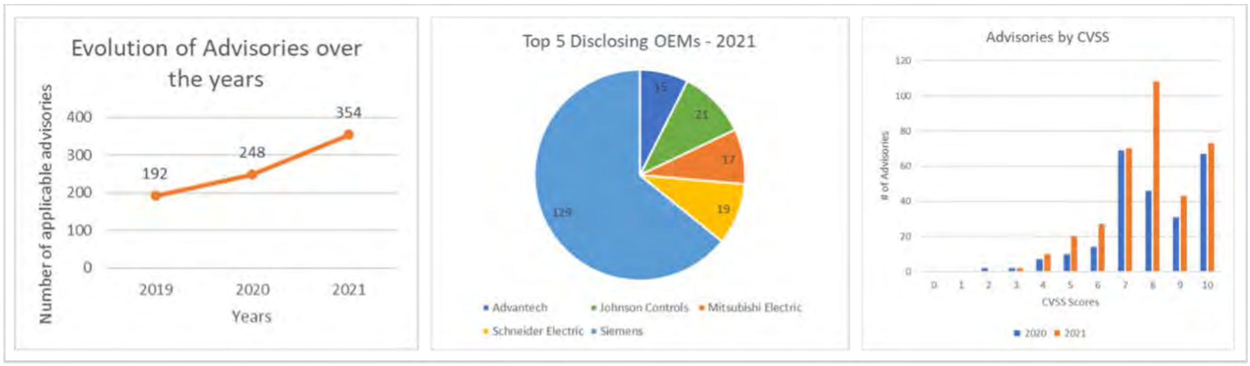
Executive Summary

In 2021, ICS-CERT issued 354 cyber security 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, size of the company, domain of operations, vendor, etc. The only advisories that were not included in the analysis were those related to medical devices (ICSMA). This report summarizes the conclusions, the observed trends, as well as a perspective on what 2022 might hold.

ICS-CERT released 354 ICS-related advisories spanning 82 vendors/ OEMs, 1,198 CVEs containing references to different products, and a matrix of affected versions.

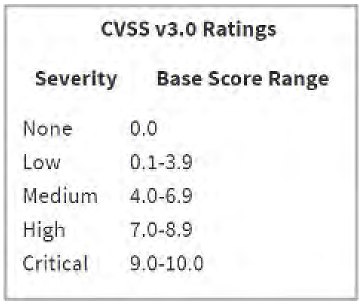
ICS-CERT advisories increased by ~30% since 2020 with the number of CVEs growing by ~41%. This compares to growth of ~23% advisories and ~32% CVEs in 2020 over 2019 in these same categories. These advisories have been split between OEM application software (51%), embedded device vulnerabilities (39%) or embedded software vulnerabilities (10%).

The OEMs/companies most affected by the ICS advisories have remained consistent since 2020, with Siemens being the OEM with the highest number of advisories to its name.



Many of the risks created by those vulnerabilities are considered High or Critical by NIST's National Vulnerability Database (NVD), with a doubling of those scored with a CVSS of 8/10 or higher since 2020.

These High and Critical vulnerabilities are generally fairly easy to exploit (67% are exploitable remotely and 75% have a low attack complexity), and with networks becoming more and more connected, the risk of lateral movement and privilege escalation is more important than ever.



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

The following trends are observed:

- Most of the vulnerabilities could be used to impact the critical manufacturing sector (59%)
- Almost half of all the reported vulnerabilities could impact more than one sector (48%)
- There is a decrease in the number of vulnerabilities affecting multiple products compared to 2020 (-20%), but still 137 advisories in 2021 that can affect multiple products
- Most of the Vulnerabilities have been identified for companies headquartered in 7 specific countries (92%)
    - This includes Germany, which can easily be explained by the fact that Siemens is headquartered there

In 2021, just like in 2020, Siemens had the largest number of advisories. In 2021, 36% of alerts were related to Siemens against 31% in 2020. 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. It shows that Siemens might actually have a relatively mature risk and vulnerability management program, and if Siemens mitigates those vulnerabilities, create patches, and helps their clients secure their products, they will be the most secure of the OEMs.

Finally, even if those vulnerabilities are important and operators, engineers, and asset owners shouldn't take them lightly, there are still several of them that contained mistakes or issues. Of the 354 ICS advisories in 2021, 27% had issues with Vendor CPE (Common Platform Enumeration).

Methodology and Data

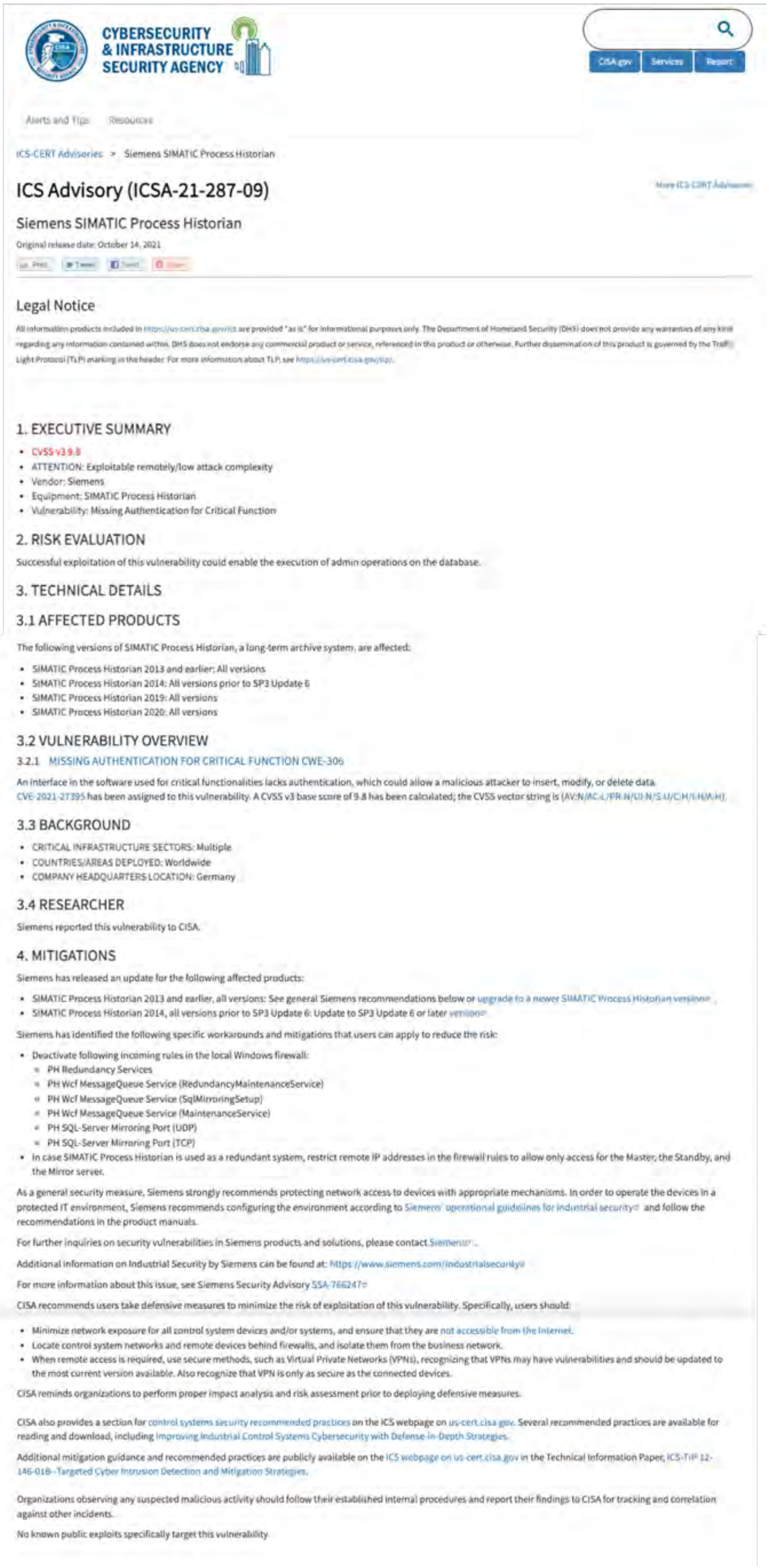
To collect data for comparison to the observations published for 2020, the Verve research team applied a similar approach:

- We collected all the ICS CERT advisory results and CVEs.
    - We removed advisories that were focused on medical devices (ICSMAs).
- We analyzed the results and reviewed for any discrepancies or gaps in the 2021 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.

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

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.


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA.gov
Services
Report
Alerts and Tips
Resources
ICS-CERT Advisories > Siemens SIMATIC Process Historian
More ICS-CERT Advisories
Print
Tweet

ICS Advisory (ICSA-21-287-09)

Siemens SIMATIC Process Historian

Original release date: October 14, 2021

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 9.8
- ATTENTION: Exploitable remotely/low attack complexity
- Vendor: Siemens
- Equipment: SIMATIC Process Historian
- Vulnerability: Missing Authentication for Critical Function

2. RISK EVALUATION

Successful exploitation of this vulnerability could enable the execution of admin operations on the database.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of SIMATIC Process Historian, a long-term archive system, are affected:

- SIMATIC Process Historian 2013 and earlier: All versions
- SIMATIC Process Historian 2014: All versions prior to SP3 Update 6
- SIMATIC Process Historian 2019: All versions
- SIMATIC Process Historian 2020: All versions

3.2 VULNERABILITY OVERVIEW

3.2.1 MISSING AUTHENTICATION FOR CRITICAL FUNCTION CWE-306

An interface in the software used for critical functionalities lacks authentication, which could allow a malicious attacker to insert, modify, or delete data.
CVE-2021-27395 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.3 BACKGROUND

- CRITICAL INFRASTRUCTURE SECTORS: Multiple
- COUNTRIES/AREAS DEPLOYED: Worldwide
- COMPANY HEADQUARTERS LOCATION: Germany

3.4 RESEARCHER

Siemens reported this vulnerability to CISA.

4. MITIGATIONS

Siemens has released an update for the following affected products:

- SIMATIC Process Historian 2013 and earlier, all versions: See general Siemens recommendations below or upgrade to a newer SIMATIC Process Historian version.
- SIMATIC Process Historian 2014, all versions prior to SP3 Update 6: Update to SP3 Update 6 or later version

Siemens has identified the following specific workarounds and mitigations that users can apply to reduce the risk:

- Deactivate following incoming rules in the local Windows firewall:
  - PH Redundancy Services
  - PH Wcf MessageQueue Service (RedundancyMaintenanceService)
  - PH Wcf MessageQueue Service (SqlMirroringSetup)
  - PH Wcf MessageQueue Service (MaintenanceService)
  - PH SQL-Server Mirroring Port (UDP)
  - PH SQL-Server Mirroring Port (TCP)
- In case SIMATIC Process Historian is used as a redundant system, restrict remote IP addresses in the firewall rules to allow only access for the Master, the Standby, and the Mirror server.

As a general security measure, Siemens strongly recommends protecting network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens' operational guidelines for industrial security and follow the recommendations in the product manuals.

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact Siemens.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

For more information about this issue, see Siemens Security Advisory SSA-766247

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or 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 that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

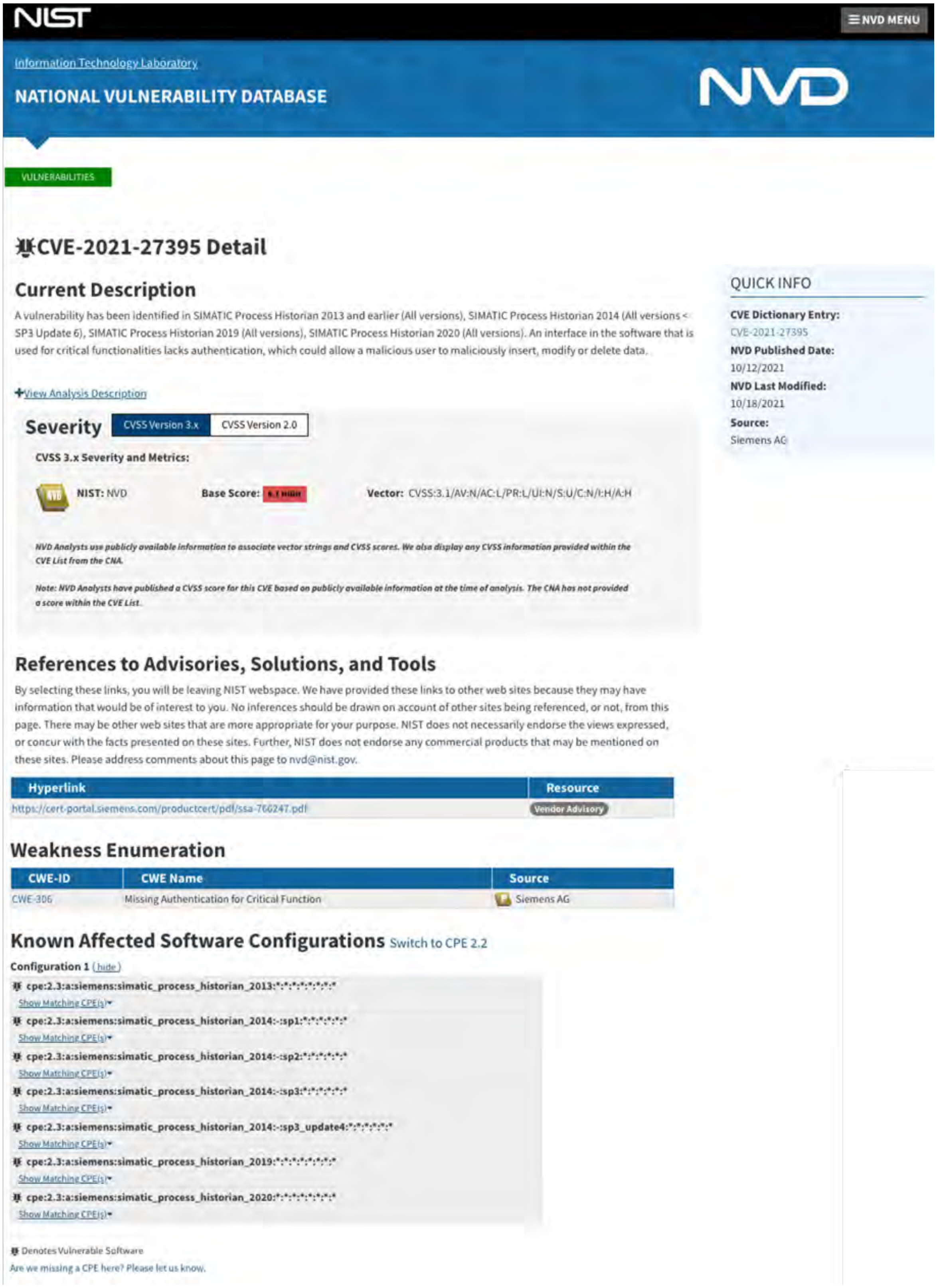
CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on us-cert.cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

No known public exploits specifically target this vulnerability.



NIST
≡ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES

CVE-2021-27395 Detail

Current Description

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.

+View Analysis Description

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 8.1 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/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: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

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://cert-portal.siemens.com/productcert/pdf/ssa-766247.pdf	Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-306	Missing Authentication for Critical Function	Siemens AG

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:siemens:simatic_process_historian_2013:*:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:a:siemens:simatic_process_historian_2014:-:sp1:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:a:siemens:simatic_process_historian_2014:-:sp2:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:a:siemens:simatic_process_historian_2014:-:sp3:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:a:siemens:simatic_process_historian_2014:-:sp3_update4:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:a:siemens:simatic_process_historian_2019:*:*:*:*:*:*:*:*
Show Matching CPE(s)▾

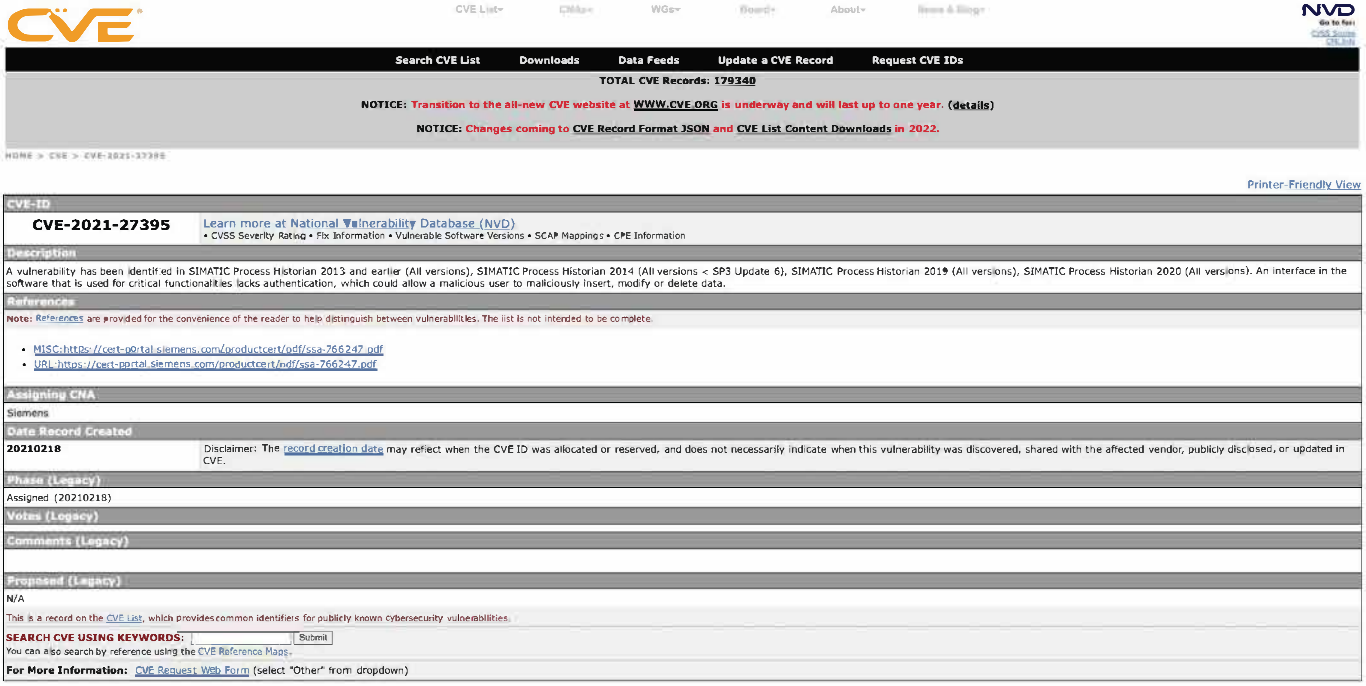
cpe:2.3:a:siemens:simatic_process_historian_2020:*:*:*:*:*:*:*:*
Show Matching CPE(s)▾

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

QUICK INFO

CVE Dictionary Entry:
CVE-2021-27395
NVD Published Date:
10/12/2021
NVD Last Modified:
10/18/2021
Source:
Siemens AG



TOTAL CVE Records: 179340

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

HOME > CVE > CVE-2021-27395

Printer-Friendly View

CVE-ID	
CVE-2021-27395	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

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.

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://cert-portal.siemens.com/productcert/pdf/ssa-766247.pdf
- URL:https://cert-portal.siemens.com/productcert/pdf/ssa-766247.pdf

Assigning CNA

Siemens

Date Record Created

20210218	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 (20210218)

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)

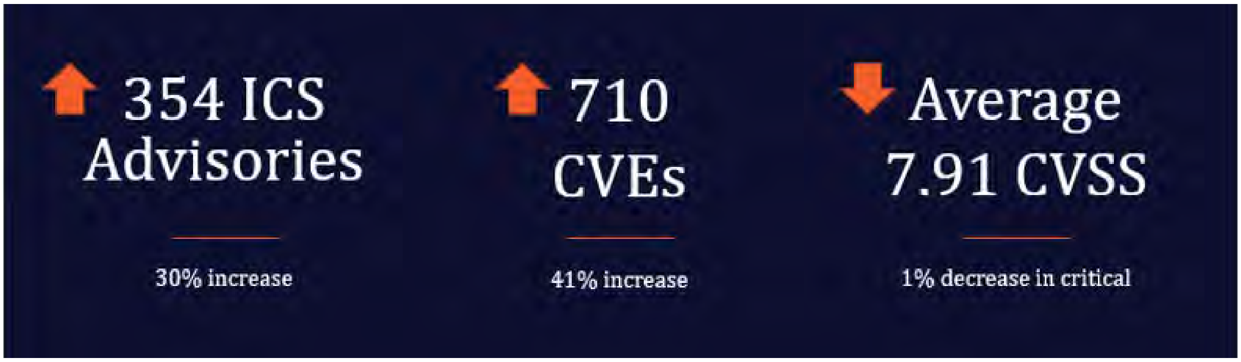
Analysis and Findings

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. These numbers show a continuing escalation in the number of ICS vulnerabilities that operators must address.

At the high level, Verve found a 30% increase in total advisories in 2021 vs. 2020 and a 41% increase in the total number of CVEs. This difference is because many advisories contain multiple CVEs. These numbers immediately highlight the challenges that industrial organizations face in ensuring their systems are vulnerability-free.

With systems/devices that often cannot be patched due to downtime or total system upgrade requirements, a general lack of inventory of assets/software/firmware/etc., and challenges when it comes to actively monitoring or scanning for vulnerabilities, ICS organizations and professionals have their work cut out for them to maintain their defenses.



354 ICS Advisories

30% increase

710 CVEs

41% increase

Average 7.91 CVSS

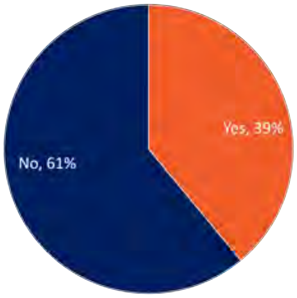
1% decrease in critical

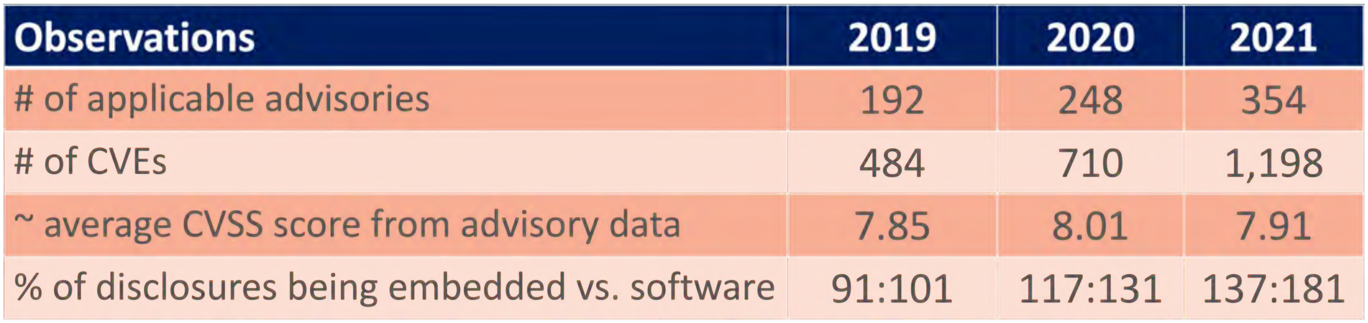
From the ~376 original ICS-CERT advisories, medical devices (ICSMA) were excluded, and with the 354 advisories that remained, they had a collective average score via the tagged CVSS of 7.91 [High]. The average number of vulnerabilities (CVEs) per advisory was also higher than one.

In addition to the above summary statistics:

- 181 were for “Software” (~51%), 137 “embedded” (~39%), 35 were both “software and embedded” (~10%), and one accounted for “other” (~0%)
- 60% were exploitable remotely with low skill or with low attack complexity, compared to 63% in 2020
- 137 affected multiple products (39%) compared to 145 (58%) in 2020, and 351 affected multiple versions (99%)

Percentage of Advisories Affecting Multiple Products

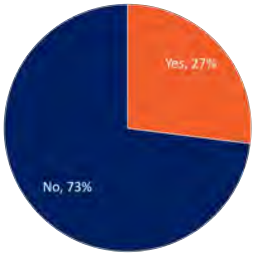




Observations	2019	2020	2021
# of applicable advisories	192	248	354
# of CVEs	484	710	1,198
~ average CVSS score from advisory data	7.85	8.01	7.91
% of disclosures being embedded vs. software	91:101	117:131	137:181

Discovery & Reporting

Number of Advisories with Issues on Vendor CPE



- 140 were self/company reported (~40%), 212 by researchers (~60%) and compared to the previous year, none of them seemed to have been identified by a government entity. Two were unmentioned/unknown (~0%).
    - The list of researchers contains independent researchers and/or members of research groups or companies that are third-party to the one targeted by the advisories.

- Some companies like Johnson Control reported a high number of vulnerabilities for their subsidiaries.

- Around 27% had issues when comparing advisory details.
    - Those issues ranged from reserved CVEs (CVE ID Not Found) to the absence of CPE in the CVE, and Third-Party CPE in the CVE, instead of the vendor ones.

Importantly, while these numbers are large and growing, this analysis does exclude 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.

The latter type of risk was highlighted recently with Vedere Labs’ release of the OT:ICEFALL vulnerability list. This release highlights the many hidden risks that exist in OT devices. Although less than 30% of these impacted industrial systems such as manufacturing, oil & gas, and utilities, the study highlights just how risky these systems can be.

This is one of the many reasons why managing risks is a complicated task. With many devices insecure by design, misconfigured, or don’t have any cyber security or compensating control around them, the fact that some vulnerabilities might not be detected or reported makes cyber security professionals’ work even more intricate.

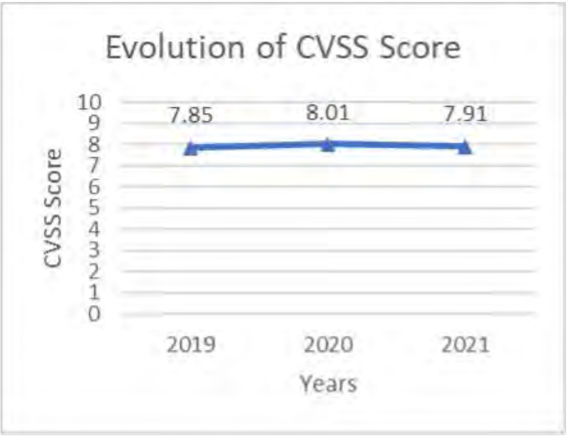
Furthermore, the debate about even these publicly released vulnerabilities creates even more confusion.

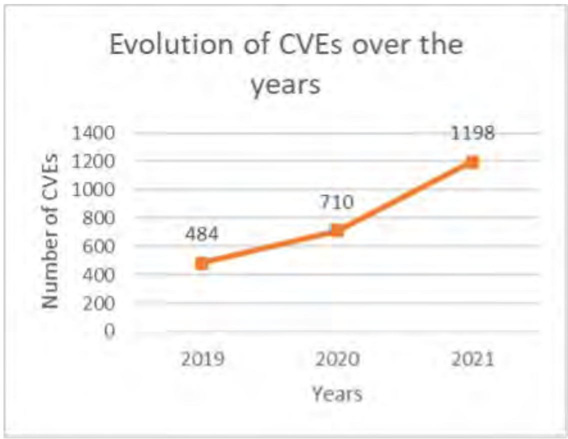
Take the recently released OT:ICEFALL vulnerabilities for example. As Eric Byres of aDolus says, "This report from Forescout is not a serious or responsible vulnerability disclosure. Not only are most of the products old and often end-of-life, but these vulnerabilities are also old news." Eric's concern is that for most, if not all of these vulnerabilities, there is no available patch or they are very old software which has been regularly updated so customers could have remediated this with regular software upgrades. His concern is that these public releases may cause more harm than good by alerting attackers to "insecure-by-design" components with no clear resolution that a vendor could take.

While vulnerability reporting is critical for asset owners to reduce risk, what's most important often gets lost in the hoopla and buzz of the latest threat. That is - to focus on the fundamentals and core principles of OT security. CISA's recommendations remain the same: Execute well across your OT systems management program, and you'll never have to worry about stopping the latest threat or chasing the shiny object.

CVSS Ratings

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





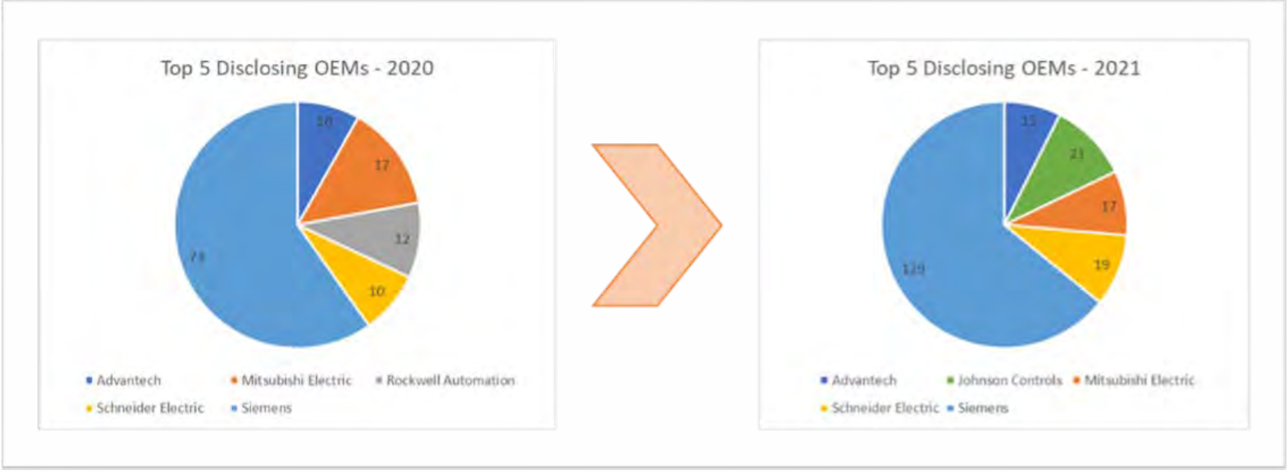
- The average CVSS Score remained consistent over the years, even as the number of advisories reported each year keeps increasing rapidly.

- On average, there were 3.38 CVEs per CVSS in 2021, which is an increase of ~0.5 CVEs per CVSS since 2020.
    - 2021 : 1198 / 354 = 3.38 CVEs per CVSS
    - 2020 : 710 / 248 = 2.86 CVEs per CVSS
    - 2019 : 484 / 192 = 2.52 CVEs per CVSS

- We took a random sample of ICS advisories to establish the level of discrepancy between the CVSS score and the suggested scores from the CVE(s) they contained. We saw some small discrepancies, but nothing major as observed in 2020. Of course, it doesn't mean that some advisories don't have major gaps between their score and the scores attributed to the CVEs they contain. Asset owners should therefore stay vigilant.
    - ICSA-21-315-12 had a CVSS score of 3.3, and 2 CVEs with scores suggested at 3.3 and 3.3.
    - ICSA-21-355-01 had a CVSS score of 10, and a total of 8 CVEs with scores ranging from 7.5 to 10. The average score of the CVEs was 9.6.
    - ICSA-21-194-06 had a CVSS score of 7.3, and one CVE with a score of 8.8. There is a small discrepancy here, but both scores are considered as high by the NVD.

Vendor Disclosures

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



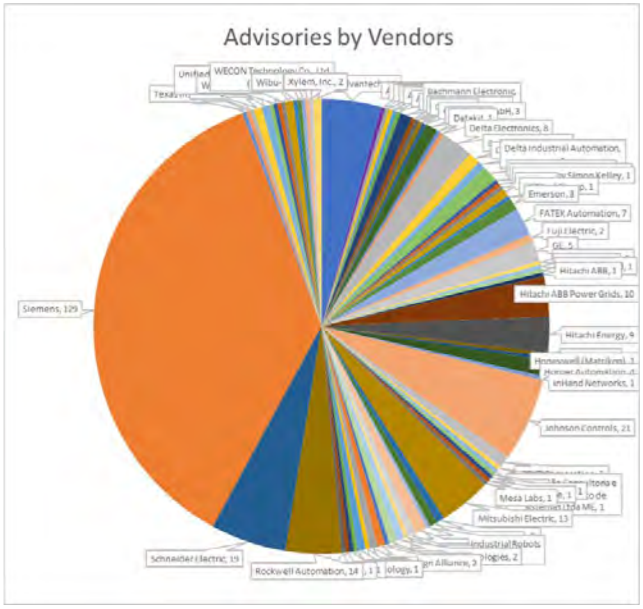
By looking at the entire data sample, it is possible to observe the following:

- Advantech notably had 15 advisories, but with a fairly high average score of 8.3 and a total of 57 CVEs.
- In comparison, Johnson Controls had 21 advisories, a lower score of 7.6, and a meager total number of CVEs of 20. Johnson Controls reported a lot of vulnerabilities for their subsidiaries, which were counted as part of Johnson Controls' statistics.
- SIEMENS has the highest number of advisories with 129 ICS advisories. They also have the advisory with the most CVEs – 43 CVEs for ICSA-21-194-15.

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

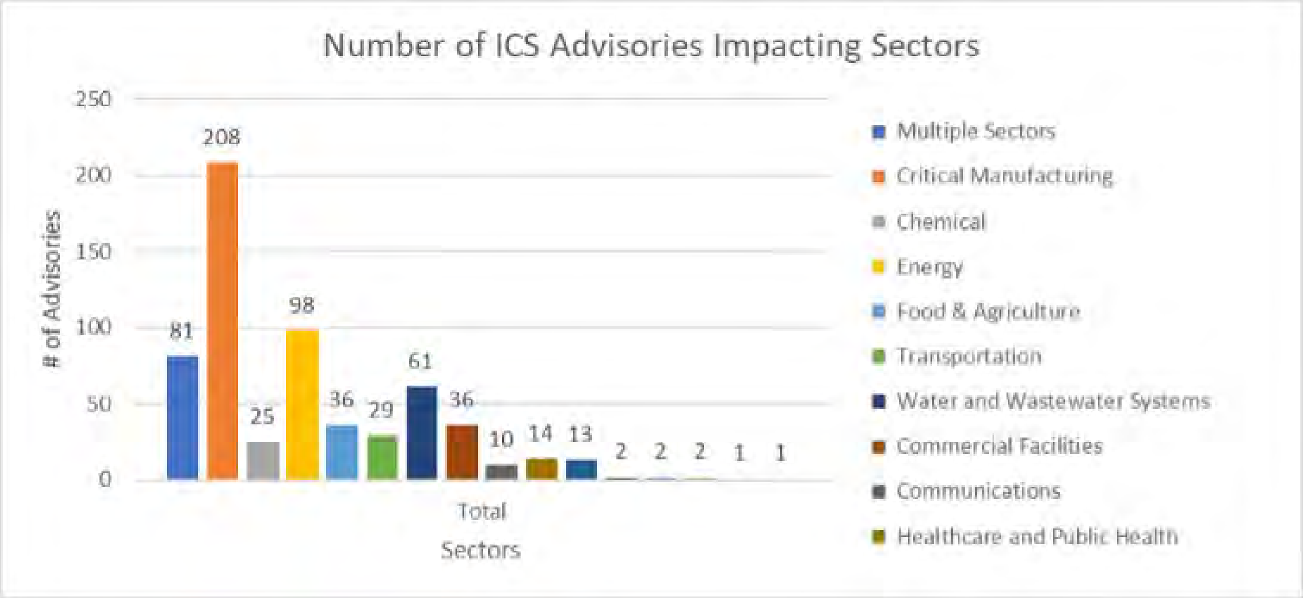
- Many vendors are not reporting vulnerabilities or sharing the vulnerabilities with affected customers. These vulnerabilities still exist but are not on the list of advisories.
- Many products impacted by the vulnerabilities are end-of-life and will not receive a patch, or another corrective measure. 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.

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.). That list of advisories is purely to help asset owners secure their environment, whether it's by patching, being more attentive and careful to what's happening out there (e.g. Monitoring), or with cyber security controls/ compensating controls.



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

- 81 advisories impact "Multiple Sectors" but do not specify which industry they touch.
- The industries with the most vulnerabilities found were critical manufacturing (59% of the advisories), Energy (28%), and Water & Wastewater Systems (17%).
- Other industries that were significantly targeted by the advisories/vulnerability found were Food & Agriculture (10%), Commercial Facilities (10%), Transportation (8%), and Chemical (7%).



The vulnerability counts are consistent with the number of attacks observed on the various "traditional" OT sectors. According to previous research done by the Verve research team, the most targeted industries in 2020 were:

- Financial and insurance (Not an OT industry)
- Manufacturing
- Energy
- Retail

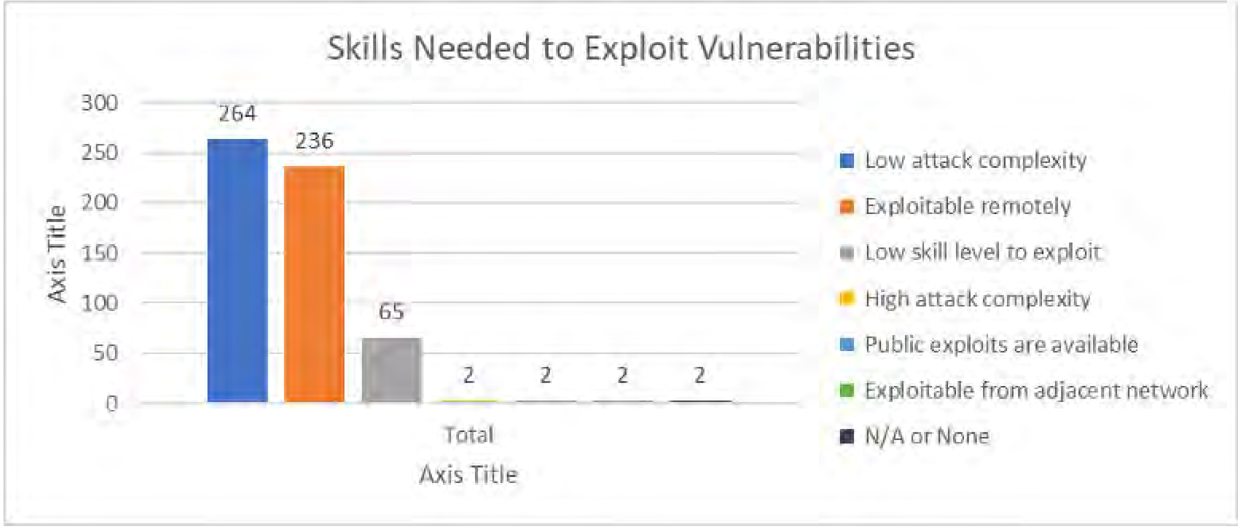
OT is clearly in the crosshairs of the cyber attackers, and manufacturing is at the center of all the OT/ICS cyber warfare game.

Top Vectors & Issues

Compared to previous years, we filtered on each skill needed to exploit vulnerabilities to obtain the full amount of CVSS that can be exploited based on specific difficulty/vector/exploit and problem/issue fields.

When we looked at the previous year (2020), we saw that 76% of the advisories could be exploited remotely. For 2021, the proportion was lower with 67% of the advisories being at risk.

The details for 2021 are presented below:



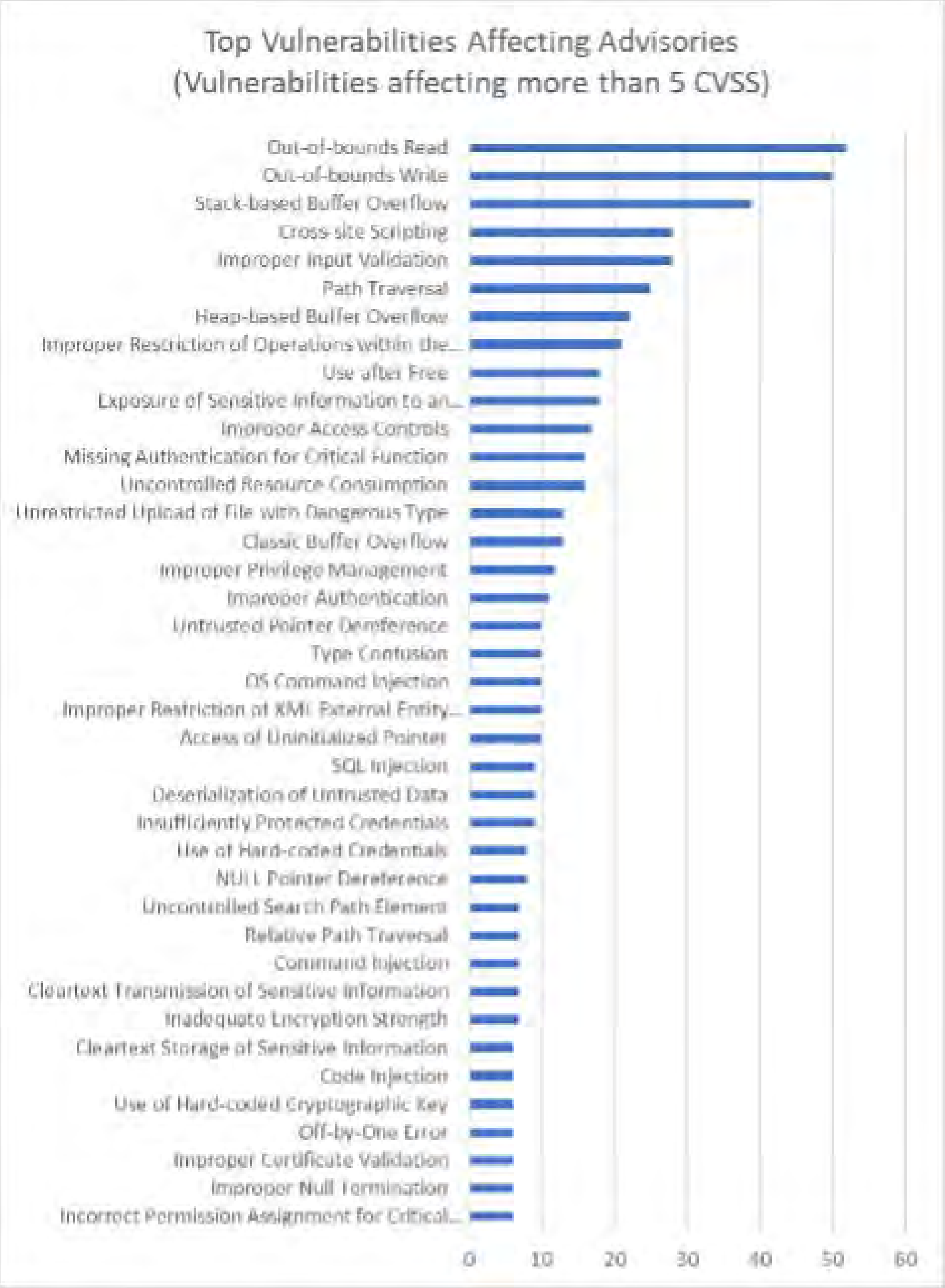
If an attacker gains access, most vulnerabilities have a low attack complexity (75%) or are exploitable with relatively low skills (18%).

161 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:

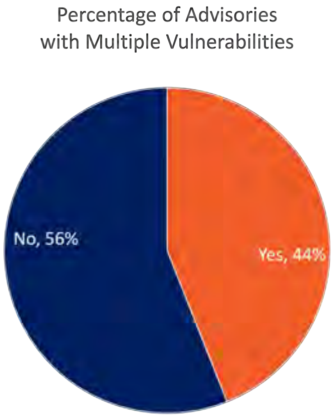
- Out-of-bounds Read: 15%
- Out-of-bounds Write: 14%
- Stuck-based Buffer Overflow: 11%
- Cross-site Scripting: 8%
- Improper Input Validation: 8%

In previous years, there may be lesser occurrence counts due to the overall numbers of CVEs being significantly lower (488 more CVEs in 2021 compared to 2020 and 226 between 2020 and 2019), and advisories (106 more in 2021 compared to 2020 and 56 more between 2020 and 2019).

However, there are similarities with 2020 when we look at the most common vulnerabilities that were reported by CISA in the ICS advisories. Buffer overflow is one of the top unique vulnerabilities for both 2021 and 2020 for example.



Top Vulnerabilities Affecting Advisories
(Vulnerabilities affecting more than 5 CVSS)



Of the 161 unique vulnerabilities that were found, 122 only affect between 1 and 5 advisories. This means that only 24% of the Vulnerabilities identified impact more than five advisories.

By adding all the vulnerabilities that impact many advisories, we got a total of 795 vulnerabilities for 354 advisories.

With that many vulnerabilities, there is a high number of advisories that have multiple vulnerabilities associated with them. According to the data collected, 44% of the advisories, so around 156 advisories, have more than one vulnerability associated with them. This is a lot and organizations need to seriously consider the ramification of having those affecting their OT/ICS operations.

Many of those vulnerabilities are without an all-inclusive fix, with many vendors offering the option to patch only a portion of the exposed products and versions, others suggesting to organizations that they upgrade their version to a more recent/latest iteration – with some specification that it will only reduce the risk and others that just don't provide any information on the impact that these upgrades would have on the vulnerability – or putting forward compensating controls such as network segmentation and firewalls.

There's even a small segment of the vendors that just decided to offer no information to CISA regarding their corresponding advisories and instead request that clients contact them directly. As such, if the threat actors targeting the organization are intentionally trying to hack into an ICS network using sophisticated means, extended resources, ICS-specific skills, and high motivation, the company may be no match against these opponents.

Remediation

The above summary can be quite scary for any controls engineer, asset owner, or cyber security executive. The number of published vulnerabilities is increasing drastically each year. To a certain extent, it can be considered a good thing as more organizations are transparent about their vulnerabilities and people are more vocal in the community. However, it also means that threat actors have a lot more information to work with to execute their attacks.

This news is a wake-up call to everyone trying to operate the critical control systems that operate so much of our economy. We need to do better to identify the vulnerabilities in our environments and eventually remediate those risks.

Remediation recommendations for these ICS vulnerabilities range from the application of specific patches or firmware updates to more mitigating measures such as ensuring configurations are reset, accounts disabled or passwords changed, or protecting network access. CISA regularly updates its guidance for OT/ICS systems with each major threat or risk announcement. And those recommendations are very consistent with security best practices. Their list includes items such as ensuring all OT/ICS devices are separated from corporate/enterprise networks, are regularly patched, have robust application whitelisting, etc. For the defenders, it is important to note these are consistent recommendations that do not evolve with each new threat. Most organizations can take heart that there is a well-defined roadmap of initiatives to provide greater security.

Based on the analysis of the ICS-CERT advisories, we recommend five key remediation actions.

First, companies should make sure 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.

- Many systems may have different constraints, and it is impossible for a company to manage their risk if they don’t know what they are protecting. Verve recommends a full inventory of the assets on the OT/ICS network and including it as part of a holistic solution that raises the visibility of these devices such that they are illuminated for actionable risk management reduction and remediation.

- Track vendor security portals to get a list of approved patches, and news of recently discovered vulnerabilities and their fixes/security updates. Use different sources to obtain vulnerability reports and integrate the information collected into the vulnerability and risk management process.
- Map vulnerabilities from various sources to identify which assets may be vulnerable in your subnets and prioritize the remediation of vulnerabilities based on criticality and your risk tolerance.

Second, organizations should assess the impact of the relevant advisories for their organizations and develop a remediation strategy to mitigate those vulnerabilities.

- Vulnerability, risk, and threat management are all interrelated and need to be closely managed and taken seriously. Organizations need a comprehensive cybersecurity management system including security assessments (high-level and detailed), prioritization of risks, vulnerability and patch management, threat intelligence, the development and implementation of controls and other means of risk reduction, training, and clear ownership of processes and systems, change management, etc.
- Organizations should identify which ICS advisories and CVEs impact them and determine the level of criticality for their environment (which device/software, role in the overall operational processes, the impact of an event/incident, etc.). A good vulnerability and risk management process is important to properly identify how the advisory affects the environment.
- Remediate the vulnerability(ies) by patching (if possible/fix available), changing a configuration, putting cybersecurity controls in place or compensating controls. Controls could include:
    - Strong password policy to access vulnerable systems
    - Protective mechanisms on the network
    - Etc.

Third, ensure OT assets and systems are protected from inappropriate actions as well as malicious application operations. 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 the protection of assets. This includes many of the CISA recommendations:

- Deploy robust network segmentation which includes both separating IT and OT networks, but also creating sub-segmentation within the OT network to provide barriers to the spread of threats that may get through the perimeter defenses.

- Deploy and lock-down application whitelisting. Whitelisting has fallen out of favor in the IT world given the frequent changes and custom application needs. In OT, however, application whitelisting is very effective given the stability of these systems.
- Ensure proper control and limitations of user and account access. This includes least privilege management, specifically eliminating dormant accounts, resetting passwords on a regular basis, removing local administrator accounts, ensuring controlled remote access to OT, etc.

Fourth, monitor the network for a potential exploit of one of the vulnerabilities.

- Understand user/access control on each device and ensure that only engineers/operators with a need-to-use basis have access to the systems. Monitor behavior on critical devices and create solid access control with restrictions based on users.
- Ensure you have resources dedicated to the monitoring of OT environments.
- Use network-based controls to monitor and secure the network from potential violation (e.g. industrial firewalls, IDS, etc.), as well as advanced means such as deep packet inspection, full OT SOC, etc.)

Fifth, ensure you’re ready to react to a potential incident linked to one of the advisories/vulnerabilities affecting the environment.

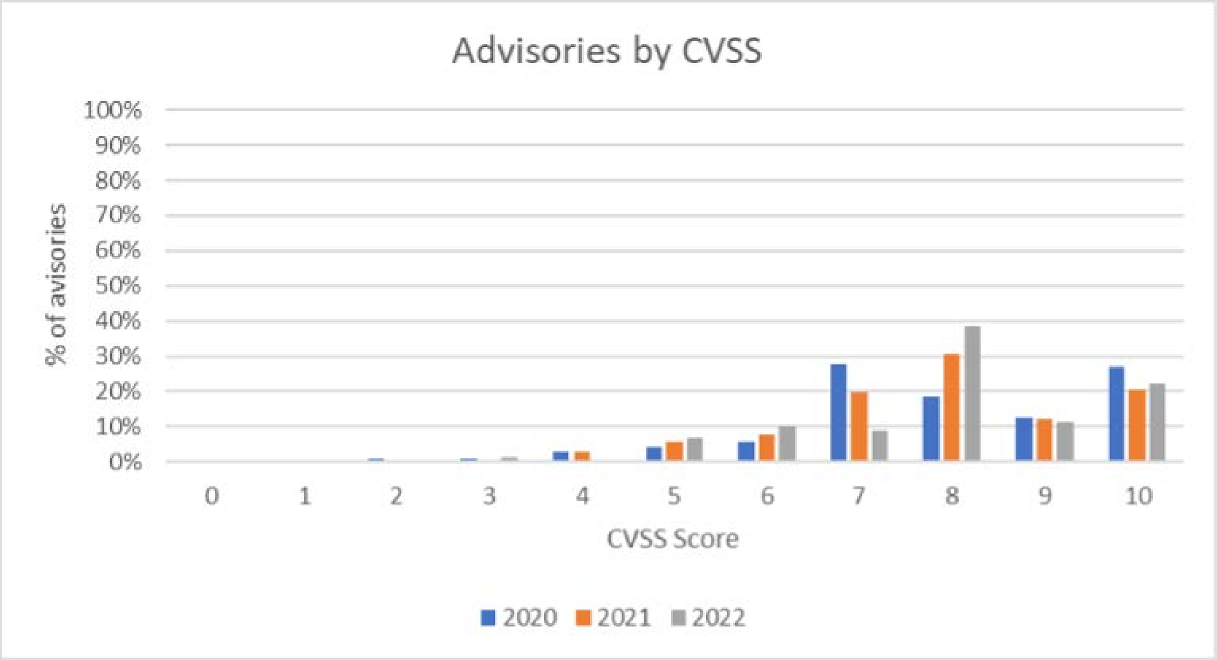
- Make sure you have a strong incident response and disaster recovery process that take into consideration the multiple risks that have been identified, as well as specific playbooks for potential violations linked to unremediated vulnerabilities.
- Ensure there is appropriate governance that both reduces risk, provides ownership and also ensures a rapid incident response.
- Perform testing activities such as tabletops, red teaming exercises, and other tests that will test the end-to-end incident response process (detection, event handling, escalation process, reporting, recovery, etc.)

Forecast & Next Steps

As of June 21st 2022, 168 ICS advisories have been published. Of those advisories, we filtered just like we did for 2021 for a comparable sample. As such, we removed 8 ICSMA (medical advisories) and rejected one advisory that didn't have an advisory rating and CVEs from the list, for a total of 159 ICS advisories.

If we compare 2021 with 2022 with similar ratios, we see the following tendencies for the current/coming year:

- In 6 months in 2022 (January to June), 159 advisories were published. In a ratio comparison to 2021 (354 advisories * 6/12 months), we see that the equivalent for 2021 would be ~177 advisories, which is slightly higher than what we have so far for 2022, but the month is not over as this analysis was completed on the 21st of June (2022).
    - 2022 could potentially end up with fewer advisories than in the previous year. This would be one of the first times the total number of advisories would decrease from one year to another based on the data we've collected since 2019.
    - However, the number of vulnerabilities/CVEs per advisory is still on the rise, with an average of 3.69 CVEs per advisory so far in 2022 and 3.38 for 2021.
- The percentage of advisories with a high criticality score seems to either stay consistent (score of 9-10) or be on the rise (score of 8).



- Siemens is still the number one OEM with the most advisories to its name. With 42% of the advisories published so far being Siemens, 2022 seems to be consistent following 2021 where advisories for Siemens were at 36%.
- The number of advisories with issues on vendor CPE seems to be on the rise so far in 2022 with 35% of the advisories having issues versus 26% in 2021. However, this number might change as the year goes on as 16 of the new advisories have CVEs currently undergoing analysis and not all information is available. A lot of CVE ID can't be found as well for the moment, but this might change as CISA compile more information on those newly issued advisories.

As observed, advisories are not going down. The year is short from over, so this number could quickly increase. With the changing situation, whether we're talking about the war in Ukraine or the evolution of the coronavirus, the number of attacks is on the rise, and the number of CVEs per advisory are growing rapidly.

What will happen with the rest of 2022 is still to be seen, but one thing is certain: organizations need to manage their risks and vulnerabilities by spending time, money, and resource on their mitigation and cyber security.

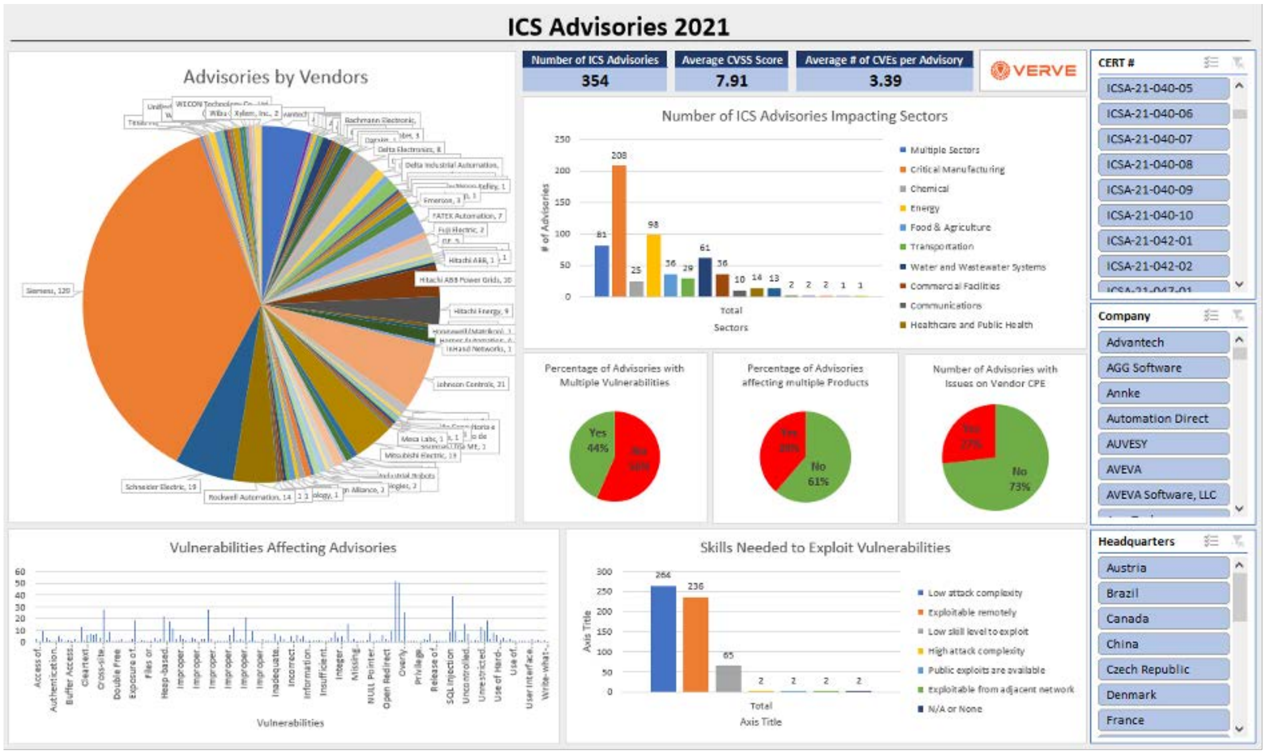
ABOUT VERVE INDUSTRIAL

With over 25 years of OT expertise, Verve Industrial is an industrial control systems cyber security company. Verve partners with clients to bridge IT OT security challenges in industrial environments.

The Verve Security Center provides robust asset inventory, vulnerability assessment, threat detection and the ability to safely remediate risks in a unified software-based platform.
Verve Industrial serves industries across utilities (such as power, oil & gas, water), manufacturing, healthcare and building controls.

Please visit us at www.verveindustrial.com to learn more.

Appendix - 2021 Dashboards



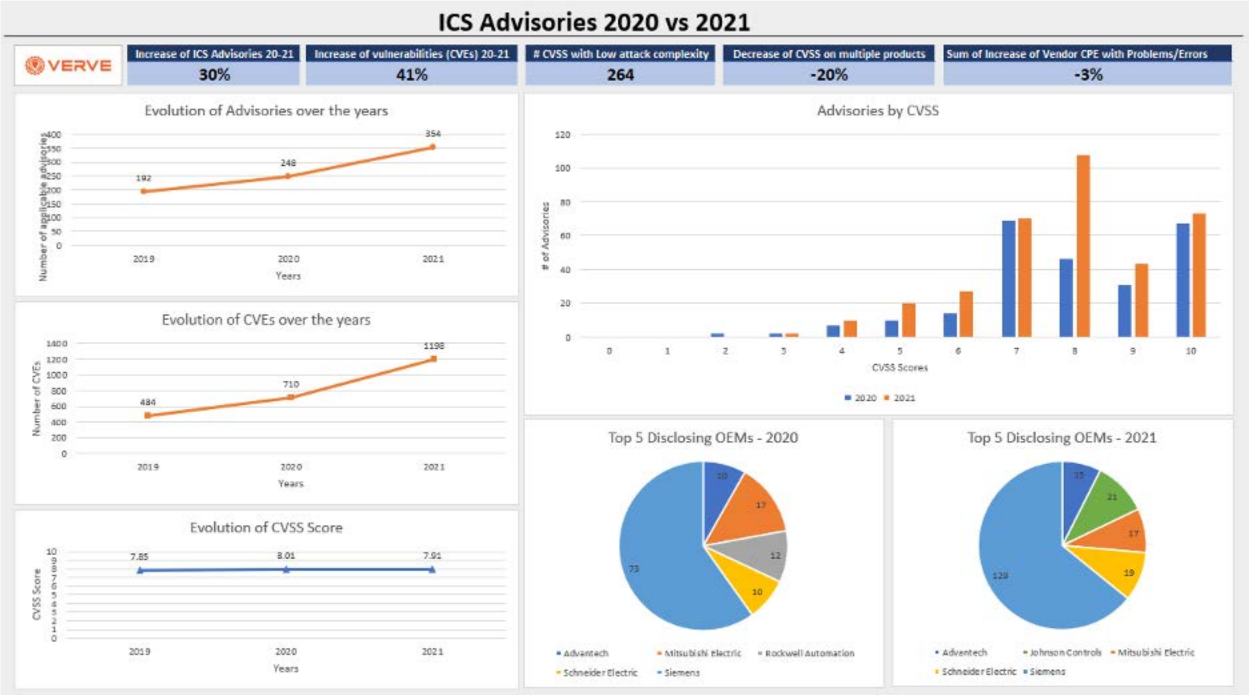
ICS Advisories 2021

Number of ICS Advisories	Average CVSS Score	Average # of CVEs per Advisory
354	7.91	3.39

CERT #: ICSA-21-040-05, ICSA-21-040-06, ICSA-21-040-07, ICSA-21-040-08, ICSA-21-040-09, ICSA-21-040-10, ICSA-21-042-01, ICSA-21-042-02

Company: Advantech, AGG Software, Annke, Automation Direct, AUVESY, AVEVA, AVEVA Software, LLC

Headquarters: Austria, Brazil, Canada, China, Czech Republic, Denmark, France



ICS Advisories 2020 vs 2021

Increase of ICS Advisories 20-21	Increase of vulnerabilities (CVEs) 20-21	# CVSS with Low attack complexity	Decrease of CVSS on multiple products	Sum of Increase of Vendor CPE with Problems/Errors
30%	41%	264	-20%	-3%