Multi-Year CVE Report

Industrial CVE Retrospective

3 Years of CISA Advisories
2020 - 2022

SYNSABER

synsaber.com

A Foreword from the CEO

Jori VanAntwerp
SynSaber CEO & Co-founder

The SynSaber team is pleased to present this comprehensive CVE (Common Vulnerabilities and Exposures) research report covering data from 2020, 2021, and 2022.

This report pulls insights from the CVEs reported as ICS (Industrial Control Systems) Advisories by CISA (the Cybersecurity and Infrastructure Security Agency) for the past three years. [Note: the data for our analysis was collected in December 2022; As CISA continually updates advisories, specific metrics may change slightly across the publication of our research reports]

As indicated in our research, the number of CVEs reported via ICS Advisories has increased each year. Vulnerability reporting was first spearheaded by ICS-CERT in the 2010s and is now managed by CISA. The ever-growing volume of reported vulnerabilities highlights continued efforts to secure the ICS systems critical to our nation's energy, manufacturing, water, and transportation infrastructure. But the growing focus and regulation come with additional administration and reporting requirements for an already overstretched ICS workforce. Owners and operators in critical infrastructure are being asked to analyze, mitigate, and report on new and existing vulnerabilities. But is the uptick in vulnerability reporting directly tied to escalating industrial threats?

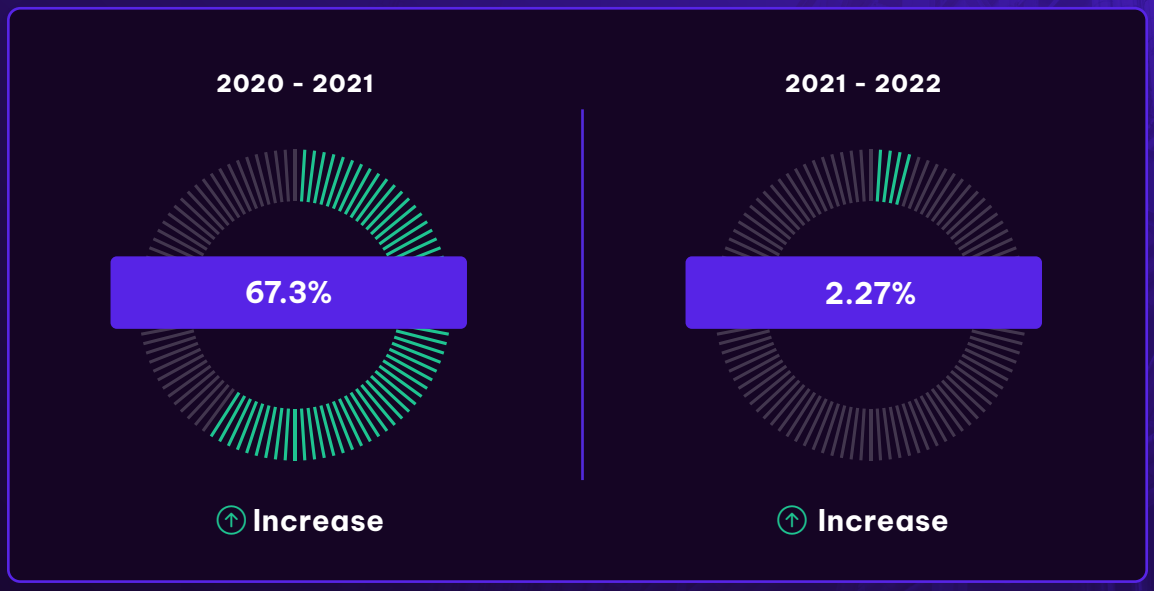
Our main goal for this report → Review the numbers and trends from the mountains of data within the ICS Advisories, and extract valuable insights that will empower critical infrastructure operators to make solid decisions regarding CVE mitigation and reporting. Fight for the operator!

Key Findings – By the Numbers

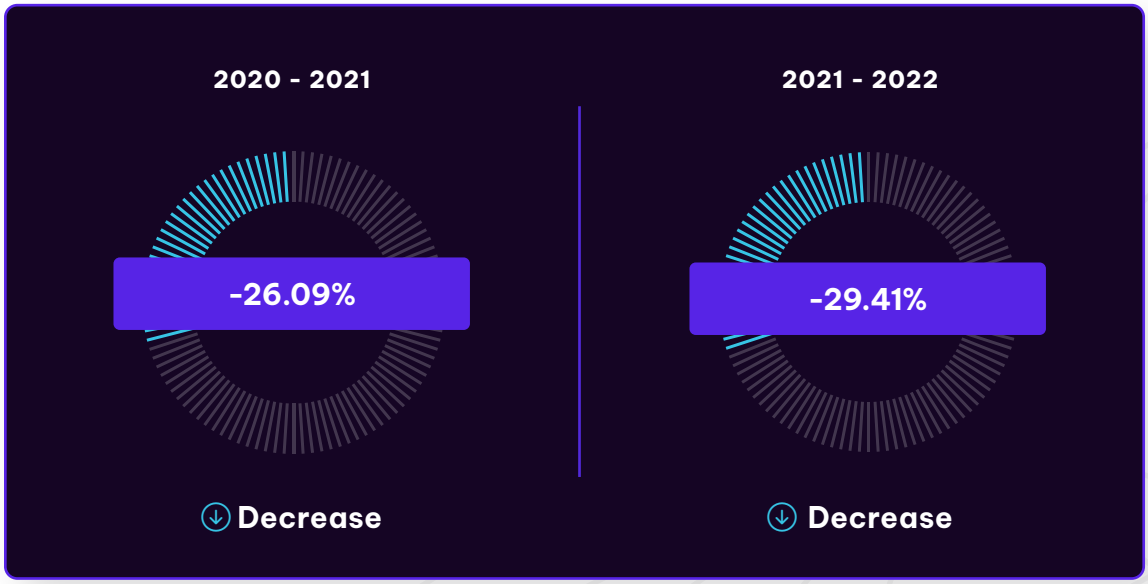
Years 2020, 2021, 2022

NOTE:
Early on, DHS ICS-CERT (CISA) began to differentiate between industrial control system advisories (ICSA) and industrial control system medical advisories (ICSMA). While medical devices are not generally considered industrial control (much like IoT), CISA includes these advisories in their reporting, so we've done the same in this report.

CISA ICS Advisory Numbers Continue to Increase

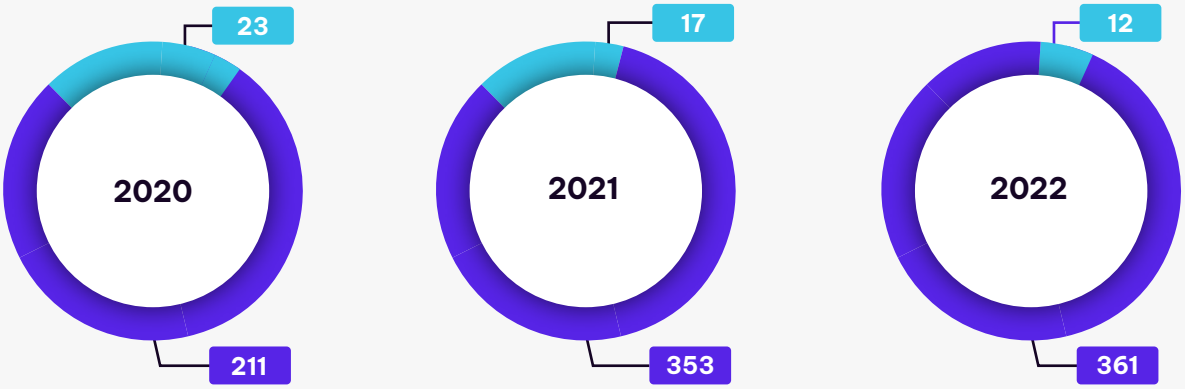


CISA ICS Medical Advisory Numbers Continue to Decrease

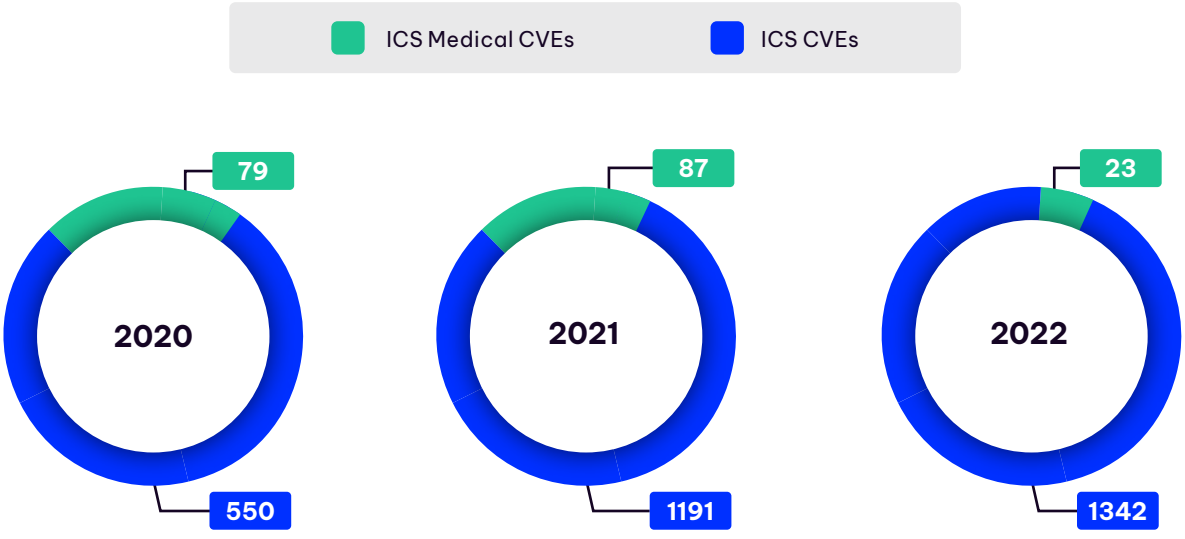


CISA Advisory Stacked Numbers 2020-2022

CISA Advisories 2020-2022



CVEs From CISA Advisories 2020-2022



Critical/High-Rated Vulnerabilities Lead

CVSS (Common Vulnerability Scoring System) Severity

While the common vulnerability scoring system may not apply perfectly to unique industrial control environments, it can be used as a prioritization method and common terminology framework across different vulnerabilities.

CVEs are scored using version 3 of CVSS across a number of criteria, such as:

ATTACK VECTOR (AV)

- Network (AV:N)
- Adjacent Network (AV:A)
- Local (AV:L)
- Physical (AV:P)

ATTACK COMPLEXITY (AC)

- Low (AC:L)
- High (AC:H)

PRIVILEGES REQUIRED (PR)

- None (PR:N)
- Low (PR:L)
- High (PR:H)

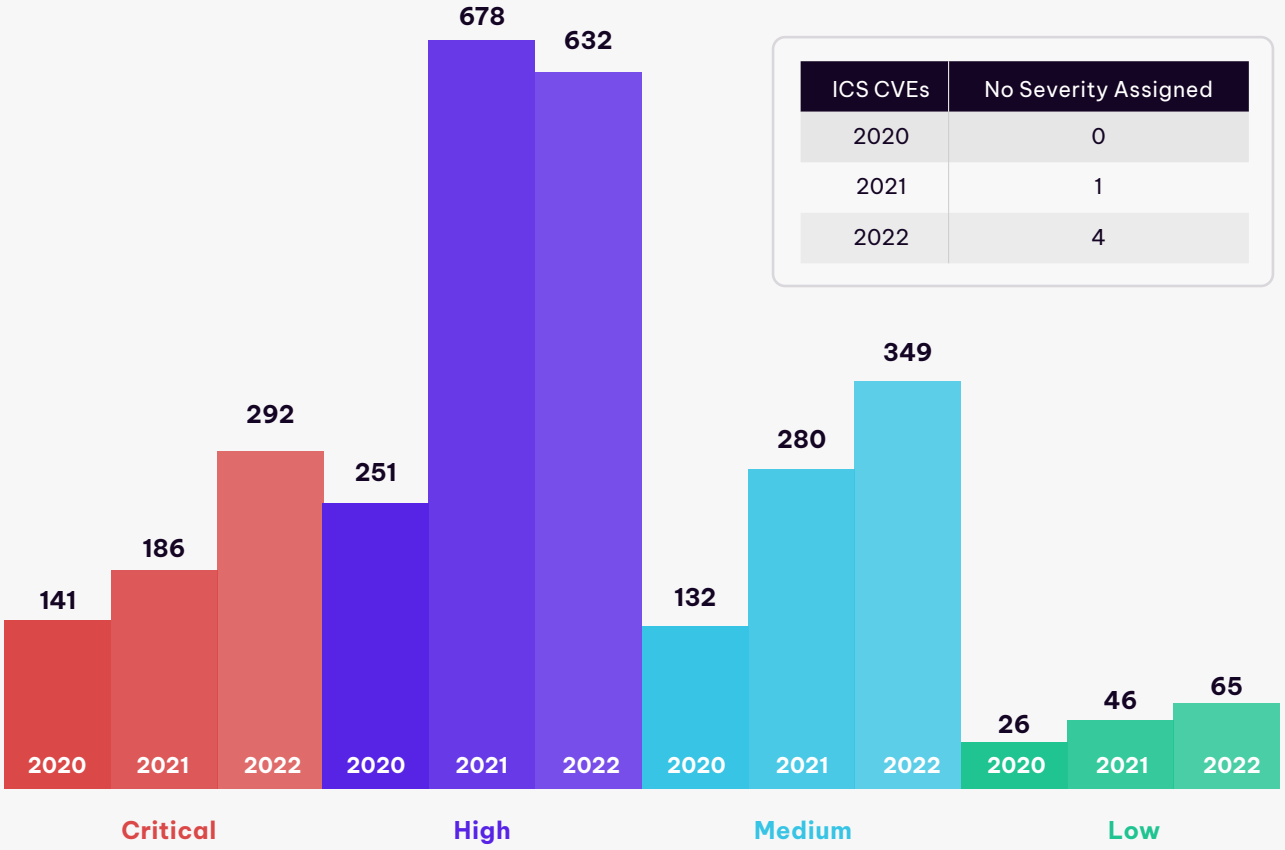
USER INTERACTION (UI)

- None (UI:N)
- Required (UI:R)

These main criteria are typically set by the CVE's vendor and, for the purposes of this report, are taken at face value. For industrial control system architectures, **Attack Vector** and **User Interaction** are of particular importance. A significant number of CVEs in industrial require Physical or Local access to the device, which can be problematic for attacks due to the physical security of industrial facilities. Requiring a user to interact with a system in order for the vulnerability to be exploited is another major hurdle.

Selecting AV:L/AV:P or UI:R impacts the scoring of the CVE. As a result, we don't see a lot of critically rated vulnerabilities in ICS. The following page contains a breakdown of CVSS severity ratings from 2020-2022.

ICS CVE Severity Stacked 2020-2022



ICS CVEs	No Severity Assigned
2020	0
2021	1
2022	4

A Significant Number of Reported CVEs have Exploit Paths that are Not Practical in ICS

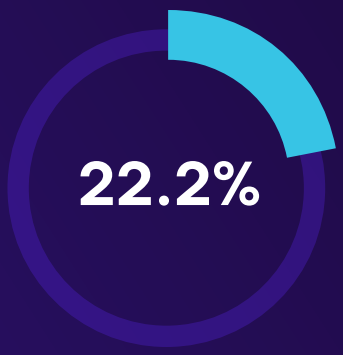
CVEs that require user interaction or local/physical access to the system are exceedingly difficult to practically exploit. Due to the nature of industrial control system operations and architecture, network accessibility and potential user interaction both have a lower probability of occurrence vs. Enterprise IT.

Common exploitation vectors like:

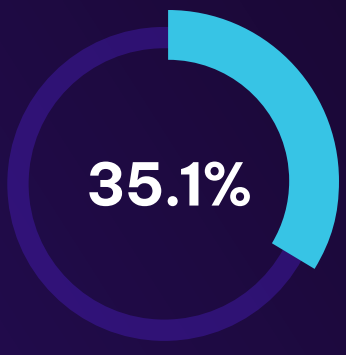
- **Direct internet access**
- **Email**
- **Web browsers**

are not typically present in industrial control environments. Given the nature of industrial built-in security, or the lack thereof, access to the industrial network equals control. Vulnerabilities are not often needed to be exploited in order to attack a process.

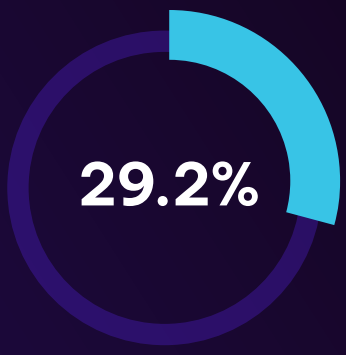
Requiring a user to interact in order to exploit is present in an average of one-quarter of all CVEs released since 2020. (22% in 2020, 35% in 2021, 29% in 2022)



ICS CVEs that Require User Interaction - 2020



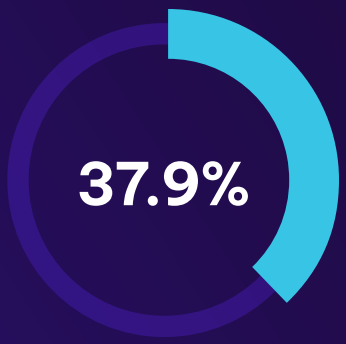
ICS CVEs that Require User Interaction - 2021



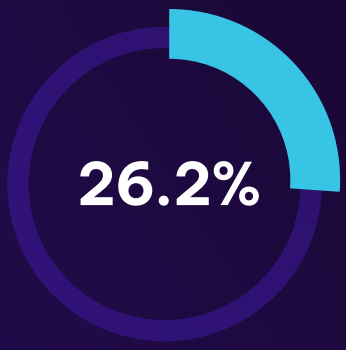
ICS CVEs that Require User Interaction - 2022

Requiring the attacker to have physical or local access to the target in order to exploit has a similar ratio of CVEs released.

ICS CVEs that Require Local/ Physical Access- 2020



ICS CVEs that Require Local/ Physical Access- 2021



ICS CVEs that Require Local/ Physical Access- 2022

Reporting CVEs

Anyone can report a vulnerability to an ICS vendor or to CISA. Whether you're an independent individual or working at one of the many ICS security companies, reporting vulnerabilities is a way to make a name for yourself and provide a service for the community.

From 2020 to 2021, there was a noticeable increase in reported vulnerabilities. Factors like the pandemic, automated tools like SBOM, or merely an increase in interest could all be contributors.

OEMS vs Security Vendors

The Sharp Rise in Reporting

When looking at pure volume, there's one name that stands out amongst the reporters: **Siemens**. But as the industrial security market grows, so does the number of CVEs reported. There's a sharp increase in security vendor interest from up-and-coming ICS-specific vendors as well as bug hunting efforts like Trend Micro's Zero Day Initiative (ZDI). Trend's ZDI disclosure process is well-defined and pays independent researchers for top vulnerabilities.

As with all CVE reporters, we again saw a sharp rise from 2020 through 2022.

OEMS

Top OEM Reporters	2020	2021	2022
Siemens	78	230	544
Hitachi	0	75	64
Mitsubishi Electric	10	37	31
Rockwell Automation	5	12	18
OEM Total	93	354	657

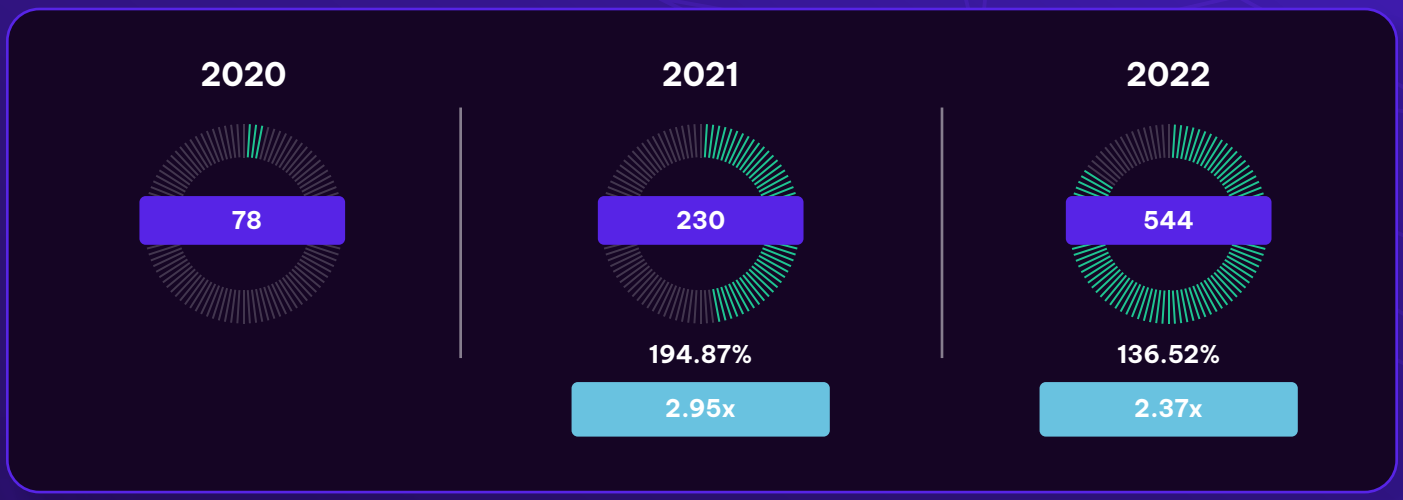
VS

SECURITY VENDORS

Top Security Vendor Reporters	2020	2021	2022
Claroty	46	97	76
Nozomi	11	16	34
Forescout	8	25	47
Trend Micro	67	246	197
Dragos	6	11	35
Security Vendor Total	138	395	389
% of Total CVEs Reported	25.09%	33.17%	28.99%

Siemens Kicks it into Gear

The team at Siemens product security continues to increase its reporting cadence with significant year-over-year growth of nearly 3x. While this does inflate the number of known CVEs that affect Siemens product lines compared to others, this should not be viewed as Siemens products being less secure. **On the contrary, a mature and repeatable OEM self-reporting process is something all other OEMs should strive to achieve.**



Cautions

Industrial Barriers to Patching

Considerations for ICS CVEs and patching — For asset owners, there are three major considerations when deciding how and when to patch, and none are related to CVSS scores or security:

WARRANTIES

Plant architectures and configurations that have passed FAT/SAT are handed over to an operator and tied to a warranty, which can prohibit changes to the industrial control system, including patching or software versions.

OEM (VENDOR) APPROVAL

If a CVE is released and a patch is available, most operating environments must wait until their OEM tests, releases, and approves the patch. This could cause a significant lag time between "patch Tuesday" and actual implementation.

MAINTENANCE WINDOWS

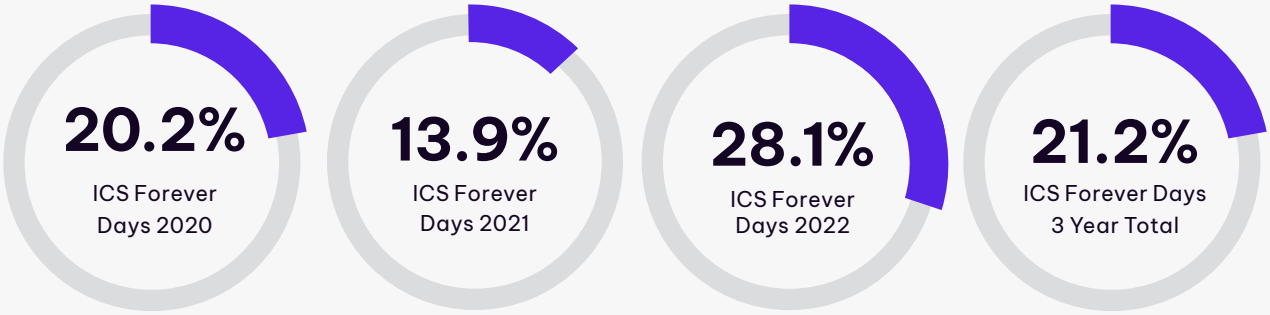
Once an OEM approves a patch, most industrial environments must wait until a prescheduled maintenance window where plant operations are shut down. This provides an opportunity for system and security patches to occur.

Some Vulnerabilities are Forever

"Forever-day vulnerabilities" is a term for vulnerabilities that are reported, but do not (and will never) have a patch available. This is more common than one might think, but many CVEs reported are for systems that are old and no longer supported. So while a new vulnerability is reported to CISA, the OEM doesn't have to release a patch or update to fix the vulnerability, leaving asset owners with limited options.

Updating the entire process to a brand-new product line is not practical, so other defensive factors or "mitigations" must be implemented.

PERCENTAGE OF FOREVER-DAY VULNERABILITIES



A QUICK REMINDER THAT FOR ICS, PATCHING MEANS:

- Downtime for the process
- Potential for "bricking" of devices
- Waiting for vendor-approved patches
- Orchestration between multiple OEMs, operators, and system integrators

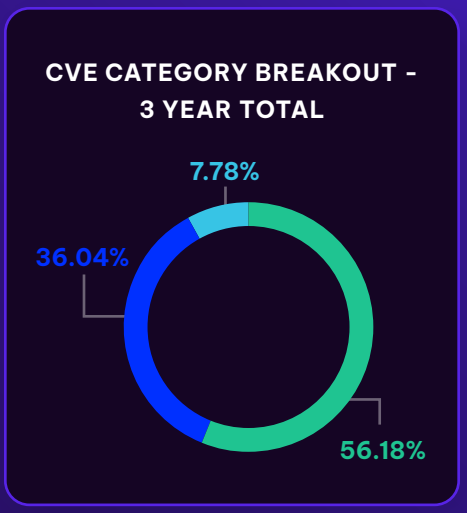
THINGS THAT CAN BE RISKY FOR ICS PATCHING:

- Automated patching
- Bulk or patching on scale
- Rapid patch pushes

Not all Patches are Created Equal

Nearly Half of all Reported CVEs Require Firmware or Architecture Updates

One does not simply patch ICS. In addition to the operational barriers to entry, there are a number of practical implementation challenges to updating industrial systems. ICS has not only software components to update but also device firmware and architectural challenges that may involve updating whole protocols. Each has a level of risk that may be considered when prioritizing activities. For example, upgrading device firmware may come with a significant risk of "bricking" the system, which could be hard to recover.



CVE Category Breakout

Using the categories of Software, Firmware, and Protocol as a basis for analysis, SynSaber has categorized each of the CVEs released in the last three years.

SOFTWARE:
The vulnerability affects a device or application and can be patched with a software update. Software patches only update the specific application.

Software	Numbers	Percentage of Total
2020	288	52.36%
2021	714	59.95%
2022	730	54.40%
Total 3 Years	1,732	56.18%

FIRMWARE:
The vulnerability affects a device or application and can only be patched with a firmware update. Firmware updates impact the entire device.

Firmware	Numbers	Percentage of Total
2020	195	35.45%
2021	387	32.49%
2022	529	39.42%
Total 3 Years	1,111	36.04%

PROTOCOL:
This vulnerability affects an entire system or architecture and may require numerous system and subsystem upgrades in order to maintain interoperability.

Protocol	Numbers	Percentage of Total
2020	67	12.18%
2021	90	7.56%
2022	83	6.18%
Total 3 Years	240	7.78%

What Should Asset Owners Do?

Criteria to Consider

Understanding that safe and reliable operation is a priority, what considerations should asset owners take into account?

3 Questions to Ask About Vulnerabilities

APPLICABLE:

Does this apply to my environment?

Without an up-to-date asset inventory, this may not be a factor easily discovered. Each CISA Advisory will have a section titled "Affected Products" that will list in some detail the exact product, software, and versions affected by the reported vulnerability.

CRITICAL:

Is this critical in the context of my environment and systems?

Although CVSS scoring shouldn't be the only indicator for prioritization (see the above Forever-Day example), it can be useful in stack ranking CVEs that meet applicability criteria.

FIXABLE:

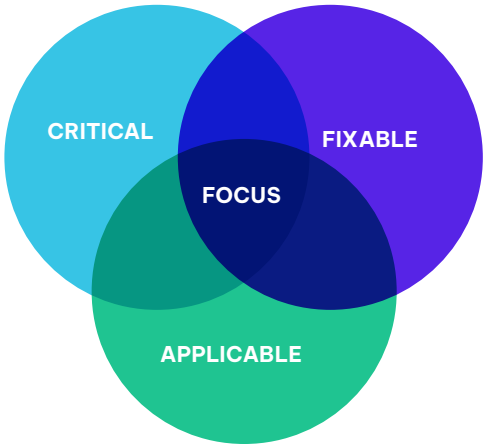
Is there a permanent fix I can deploy in my environment?

This category can be very complex, as industrial systems may not have straightforward patch management capabilities like in enterprise environments.

Fixable, in this case, is a combination of criteria that include:

- Software patch, firmware, or upgrade available from the OEM
- Configuration that is attainable and not disruptive to operations
- Doesn't require a whole system, subsystem, or architecture change

Focus When Applicability, Criticality, and an Available Fix Intersect



ICS Vulnerability Timing and Focus

Applying the information we have (such as remediation availability, impact, criticality, and other metrics) to the CVEs reported from 2020 through 2022, we've grouped them according to timing and focus:

NOW

This group includes CVEs that (with organization and vendor planning) can and should be addressed immediately.

NEXT

These CVEs are more complex from a remediation perspective but still require attention. Examples include firmware updates that could affect a large number of fielded devices.

FOREVER

These are CVEs that have architectural and interoperability impacts. One cannot simply patch away a protocol vulnerability, or upgrade an entire SCADA.

Categorizing vulnerabilities in this manner doesn't mean all CVEs should be ignored. Recognizing the barriers to patching in ICS and other practical considerations, the intent here is to represent a huge amount of data in a way that communicates calm. Even if a CISA-advised CVE is applicable, it does not necessarily mean emergency action is required. Each security and industrial operator must go through an evaluation process in order to determine the best actions.

Focus Categories	3 Year Total	Percentage of Total
Now	998	32.4%
Next	1618	52.5%
Forever	467	15.1%

In Conclusion

The volume of CVEs reported via CISA ICS Advisories and other entities is not likely to decrease. It's important for asset owners and those defending critical infrastructure to understand when remediations are available, and how those remediations should be implemented and prioritized.

Merely looking at the sheer volume of reported CVEs may cause asset owners to feel overwhelmed, but the figures seem less daunting when we understand what percentage of CVEs are pertinent and actionable vs. which will remain "forever-day vulnerabilities," at least for the time being. Does an increase in reported CVE numbers indicate any of the following?

- Industrial control system security is trending downwards
- Industrial threats are trending upwards

Not necessarily. What it could indicate is that product security teams are increasing their internal reporting and public disclosure of vulnerabilities to the community. More transparency is typically a great thing when it comes to vulnerability research, but the community at large must be cautious and skeptical of companies or individuals running up the numbers for the sake of fame and fortune. Understanding the overall metrics, analysis methodologies, and considerations of ICS CVEs is a great step toward empowering our industrial community and fighting for the operator!

FIGHT FOR THE OPERATOR

SynSaber will continue monitoring and analyzing reported CVEs, and we will update this research as new trends and key findings arise. If you have any questions about this research, or would like to learn more about SynSaber, you can reach us at info@synsaber.com or synsaber.com/contact-us.

Terms • Definitions • Notes

RESEARCH SCOPE

- Metrics are limited to CVEs as reported by CISA ICS Advisories
- Time period: 1 January 2020 - 31 December 2022
- Data was collected in December of 2022, with many CISA advisories updated throughout 2022. Note that CISA continually updates advisories as required, so specific metrics may change slightly after report publication.
- Includes CVEs first discovered outside of the time period but newly applied to ICS via CISA ICS Advisories
- Common Vulnerability Scoring System (CVSS) scores are taken at face value. Note that CVSS scores may change over time as vulnerabilities are reevaluated by the reporter and affected vendor.
- A small number of reported CVEs had multiple data points per field, like CVE reporters. A single data point was used for overall metrics analysis but did not significantly change the outcome.

CVSS

CVSS is a vulnerability scoring mechanism used in the community to categorize and prioritize through a quantifiable rating system. This scoring is at the submitting party's discretion and is often inaccurate within ICS environments.

Terms • Definitions • Notes

CVE CATEGORY BREAKOUT

Software: The vulnerability affects a device or application and can be patched with a software update. Software patches only update the specific application.

Firmware: The vulnerability affects a device or application and can only be patched with a firmware update. Firmware updates impact the entire device.

Protocol: This vulnerability affects an entire system or architecture and may require numerous system and subsystem upgrades in order to maintain interoperability.

CVSS ATTACK VECTORS

For our purposes, Local/Physical metrics have been combined.

Network: The vulnerable component is "remote exploitable" via network attack that can be routed through one or more hops (across network segments, OSI Layer 3)

Adjacent: The vulnerable component is remote exploitable but must be launched from the same local subnet (OSI Layer 2)

Local/Physical: The vulnerable component is exploited only at the local level, requiring either direct physical access or user interaction

SYNSABER

FIGHT FOR THE OPERATOR

SynSaber is the simple, flexible, and scalable industrial asset and network monitoring solution that provides continuous insight into the status, vulnerabilities, and threats across every point in the industrial ecosystem, empowering operators to observe, detect and defend OT/IT systems and protect critical infrastructure. Navigate your security quest with confidence.

synsaber.com