

Research Report

ICS Vulnerabilities

SynSaber Analysis,
First Half of 2022



synsaber.com

Copyright © SynSaber

Introduction





With increased discussion around industrial control system (ICS) vulnerabilities, we at SynSaber wondered: What if we looked at reported Common Vulnerabilities and Exposures (CVEs) from a different perspective. What questions could be answered from the 681 CVEs reported via the Cybersecurity and Infrastructure Security Agency (CISA) ICS Advisories in the first half of 2022?

Given the unique nature of industrial control system environments, not all vulnerabilities may be equally critical or even patched. What are asset owners and their security teams to do?

Breaking up the reported CVEs into remediation categories (i.e., can it be patched with software, a firmware update, or something more complex requiring protocol or whole system changes) or taking a look at attack vector requirements can provide critical insights for teams to assess these and future CVEs as they are reported.

While not all CVEs may apply to your specific industrial environments, we hope that by analyzing and counting these vulnerabilities with new methods, this context can be used by all industrial security teams to better understand and remediate future vulnerabilities.

Our researchers sought to answer questions like:

-  **Who is reporting the majority of CVEs?**
-  **What number of CVEs have a low probability of exploitation?**
-  **Given the reported CVEs, what remediations are available (if any), and how difficult is it for asset owners to fix?**
-  **Overall, what percentage of reported CVEs matter?**



Key Findings

For the CVEs reported in 2022,

13%

have no patch or remediation currently available from the vendor
(and 34% require a firmware update)

While 56% of the CVEs have been reported by the Original Equipment Manufacturer (OEM),

42%

have been submitted by security vendors and independent researchers
(remaining 2% were reported directly by an asset owner and a government CERT)

23%

of the CVEs require local or physical access to the system in order to exploit

Of the CVEs reported thus far in 2022,

41%

can and should be prioritized and addressed first
(with organization and vendor planning)

Key Insights

1

**Identifying Low
Probability of Exploitation**

2

**What Can
Be Done?**

3

**Who is
Generating CVEs?**

Identifying Low Probability of Exploitation

You can determine if a vulnerability is practically exploitable within your ICS environment by looking at certain key measures. Network accessibility and potential user interaction both have a lower probability of occurrence in ICS vs. Enterprise IT.

Example CWE

Plaintext Storage of a Password CWE-256

(see <https://cwe.mitre.org/data/definitions/256.html>)

\$DEVICE stores credentials in plaintext on the system flash memory.

In this example, the attacker must have physical access to the device and be able to interact with the system flash memory in order to gain access to plaintext passwords. It's possible that an attacker may acquire or steal a device, extract passwords from flash memory, and then reuse those credentials for an attack. These chains of events require physical and logical access along with other caveats.

Example CWE

Improper Neutralization of Input During Web Page Generation ('Cross-Site Scripting') CWE-79

(see <https://cwe.mitre.org/data/definitions/79.html>)

In certain configurations, the SAML module is vulnerable to cross-site scripting (XSS) attacks due to insufficient error message sanitation. This could allow an attacker to execute malicious code by **tricking users into accessing a malicious link.**



46 of 681 (6.75%)

require both Local/Physical and User Interaction for the vulnerability to be successfully exploited.



198 of 681 (29.07%)

require User Interaction regardless of network availability.

KEY INSIGHT #1

Phrases to look for
in ICS Advisories:



“Without validation, an admin user could be tricked to install a malicious package, granting root privileges to an attacker.”



“Successful exploitation of this vulnerability could allow a malicious user to trick a legitimate user into using an untrusted website.”



“Allowing users with SYSTEM/ROOT/ADMIN/ELEVATED level privileges to perform \$ACTION.”

What Can Be Done?

If a CVE cannot be patched in the forest, does it make an exploitable sound?
What practical fix actions are available for CVEs?

These “fix” actions could be:



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.

Or perhaps there is no fix, the dreaded “Forever-day Vulnerability” that the vendor says will never be patched.

Breakout of CVE Action Types

	Count	Percentage of Total (681)
■ Software	361	53.0%
■ Firmware	235	34.5%
■ Protocol	85	12.5%



KEY INSIGHT #2

Generally speaking, even if there is a software or firmware patch available, asset owners are still required to work with the affected Original Equipment Manufacturer (OEM) vendor and wait for official approval to patch.

This is due to complicated interoperability and warranty constraints that apply to industrial control systems. Just because a patch exists doesn't mean an organization can immediately apply it. Aside from OEM restrictions, organizations must determine the operational risk and follow internal configuration management policies and procedures.



Just because a patch exists doesn't mean an organization can immediately apply it.

Who is Generating CVEs?

It's important to point out that the most prolific CVE generator was Team Siemens, with 230 CVEs, or one-third of the total reported for the first half of 2022. Go, Siemens! OEMs reported a combined total of 384 CVEs, or 56% of all reported. OEMs are the product vendors in which the vulnerabilities exist, and their security teams have access to the business units, software, and developers of the vulnerable systems. Therefore, they should typically be generating the most meaningful and accurate CVEs out of the bunch.

Compania Minera Dona Ines de Collahuasi S.C.M., a mining company out of Chile, reported four vulnerabilities (<https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-03>) in Hitachi Energy LinkOne WebView. While these vulnerabilities won't be given a cool name and logo, it's encouraging to see asset owners both discovering and working with vendors to remediate vulnerabilities.

Another mention; **JPCERT** (Japan's National CERT) reported five vulnerabilities in Yokogawa CENTUM and ProSafe products to CISA (<https://www.cisa.gov/uscert/ics/advisories/icsa-22-123-01>).

Security vendors and independent researchers reported 288 CVEs during the first half of 2022, or 42% of the total.

That other 2%

of reported CVEs were from an Asset Owner and Government CERT (see left).



KEY INSIGHT #3

But wait,

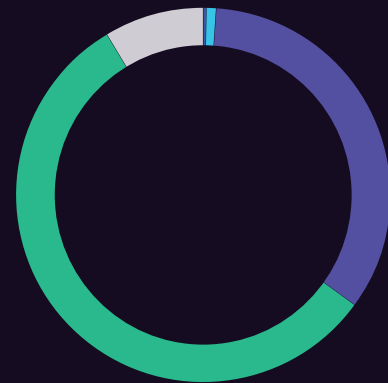
when looking at Yokogawa’s advisory linked on the CISA page (<https://web-material3.yokogawa.com/1/32463/files/YSAR-22-0004-E.pdf?ga=2.245343553.530057536.1650301120-1779617245.1650301120>), we see that the Yokogawa acknowledges “**FSSTEC of Russia**” (https://en.wikipedia.org/wiki/Federal_Service_for_Technical_and_Export_Control).

Intriguing!

- **OEMs like**
Siemens, Mitsubishi Electric
- **Security Vendors like**
Trend Micro, Claroty
- **Independents**
- **Asset Owners**
Compania Minera Dona Ines de Collahuasi S.C.M., a mining company out of Chile
- **Government**
JPCERT

Breakout of CVE Action Types

	Count	Percentage of Total (681)
■ OEM	384	56.4%
■ Security Vendor	231	33.9%
■ Independent	57	8.4%
■ Asset Owner	4	0.5%
■ Govt	5	0.7%



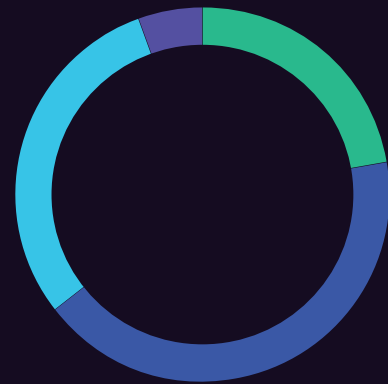
...Security teams have access to the business units, software, and developers of the vulnerable systems.

Additional Metrics

In addition to the key insights listed previously, SynSaber researchers were able to pull out additional metrics and key findings from the CVE Advisories that have been released by CISA during the first half of 2022.

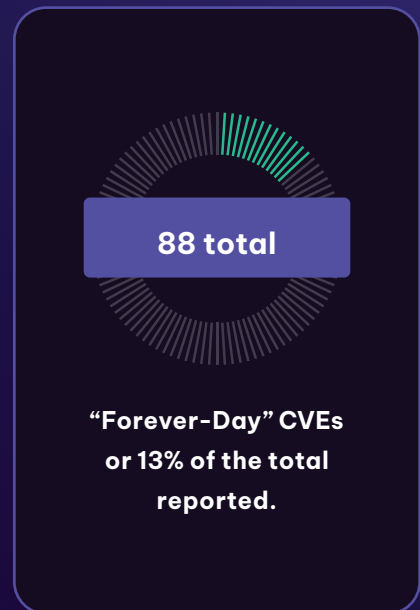
CVEs by CVSS Criticality

	Count	Percentage of Total (681)
■ Critical	152	22.32%
■ High	289	42.44%
■ Medium	205	30.10%
■ Low	35	5.14%



Looking at just Critical / Highs and breakout of type, how many CVEs do not have a patch? (“Forever-Day” Vulnerability)

	Has Patch	No Patch	Percentage no Patch
Critical / Software	114	2	1.72%
Critical / Firmware	20	8	28.57%
Critical / Protocol	5	3	37.50%
High / Software	116	18	13.43%
High / Firmware	91	20	18.02%
High / Protocol	41	3	6.82%



CVEs that Require User Interaction

29%

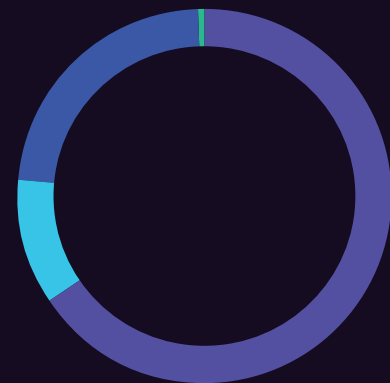
of reported CVEs require the user (operator) to do something in order for exploitation to occur [relevant to Key Insight #1 regarding probability of exploitation]

ADDITIONAL METRICS

CVEs that Require Access

In industrial networks, access = control. While we are at the mercy of whatever the reporter and vendor assign for the CVSS Attack Vector category, **154 (22.61%) of reported CVEs require local or physical access** to the system in order to exploit. If you have local/physical access, often no exploit is required. The same can be said for most network-based CVEs, although it does not diminish the importance of the CVE itself.

	Count	Percentage of Total
■ Network	437	65.6%
■ Adjacent	73	11.0%
■ Local/Physical	154	23.1%
■ Unknown/Unassigned	2	0.3%



Overall CVE Focus?

What organizations should focus on is a complex blend of risk and HAZOPS (Hazard & Operability Studies; <https://synsaber.com/cyber-risk-quantification-and-hazops/>) assessments, ability to fix, vendor approvals, and other factors too difficult to simply assign scoring.

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

277 40.7%

345 50.7%

59 8.7%

- **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 environment. Organizations may be dealing with these CVEs for a long time, and other compensating controls will likely be required.

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.


SynSaber plans to 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 Jan to 30 June, 2022

 Common Vulnerability Scoring System (CVSS) scores taken at face value

CVSS

CVSS is a vulnerability scoring mechanism used in the community to categorize and prioritize through a quantifiable rating system (<https://www.first.org/cvss/calculator/3.1>). This scoring is at the submitting party's discretion and is often inaccurate within ICS environments.

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.com

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.