

Research Report

ICS Vulnerabilities

SynSaber + ICS[AP] Analysis,
First Half of 2023



SYNSABER ICS[AP]

Copyright 2023 © SynSaber + ICS[AP]

Introduction

SynSaber is excited to partner with the ICS Advisory Project in our continued analysis of ICS Advisories reported by the Cybersecurity and Infrastructure Security Agency (CISA). We sought to find and evaluate notable trends in Common Vulnerabilities and Exposures (CVEs) to see what OT and ICS asset owners should be aware of.

With the growing regulation around critical infrastructure and the industrial control systems that constitute them, there is increasing emphasis around maturing cybersecurity and operations, resulting in increased efforts around vulnerability management.

While not all CVEs may apply to each industrial environment, we hope that by analyzing these vulnerabilities, these methods and tools can be used by industrial security teams to better understand and remediate future vulnerabilities.



As a team, we sought to answer questions like:



How has the number of CISA-reported ICS CVEs changed in comparison to the first half of 2022?



What is the spread of CVEs across software, hardware, or other vulnerabilities?



Where are the majority of reported CVEs originating from?



How should asset owners and operators prioritize reported CVEs?

Key Findings Summary

The total number of CISA ICS Advisories has decreased

9.8%

compared to the first half of 2022. This could be attributed to more CVEs being listed per advisory.

The total number of reported CVEs has decreased

1.6%

compared to the first half of 2022. (Reminder: this report and any comparisons are primarily focused on the CVEs that were reported in CISA ICS Advisories)

For the CVEs reported in the first half of 2023,

34%

have no patch or remediation currently available from the vendor (significantly up from 13% in the first half of 2022, but fairly consistent with the 35% from the second half of 2022).

OEMs

remain in the lead as the top CVE reporters. Siemens, Trend Micro's Zero Day Initiative (ZDI), and Hitachi are the top CVE reporters included in CISA ICS Advisories.

**MANUFACTURING
AND ENERGY**

(37.3% and 24.3% of total reported CVEs respectively)
were the two sectors most likely to be affected by the CVEs that were reported in the first half of 2023.

Key Insights Covered

1

The CVE Numbers and Details

2

Who is Reporting CVEs?

3

Who is Most Impacted?

4

Probability of CVE Exploitation

The CVE Numbers and Details

| CVEs reported via CISA ICS Advisory | 1H23 | 1H22 | Difference |
|-------------------------------------|------|------|------------|
| Total CVEs Reported | 670 | 681 | ▼ 1.6% |

In comparing the total number of CVEs appearing in CISA ICS Advisories in the first half of 2023 to those reported in 1H22, there has been a slight decrease of 1.62%.

| CISA ICS Advisories | 1H23 | 1H22 | Difference |
|----------------------------------|------|------|------------|
| Total CISA ICS Advisories | 185 | 205 | ▼ 9.8% |

Both the number of CVEs and total CISA ICS Advisories have decreased from the first half of 2022 compared to the first half of 2023, though there has been a greater decrease in the number of advisories than the total number of CVEs.

This could be attributed to multiple CVEs being reported within individual ICS Advisories, as CISA streamlines its alert & reporting processes. One [Siemens report](#), for example, included over 100 CVEs.

| Breakout of CVE Action types | 1H23 Count | 1H23% | 1H22 Count | 1H22% |
|------------------------------|------------|-------|------------------------|-------|
| Software | 276 | 41.2% | 361 | 53% |
| Firmware | 178 | 26.6% | 235 | 34.5% |
| Other | 216 | 32.2% | (variant data in 2022) | |

There has been a slight decrease in the percentage of Software and Firmware action types for ICS CVEs reported in the first half of 2023 (action type descriptions can be found in the “Terms, Definitions, and Notes” section at the end of this report).



THE ONES THAT GOT AWAY!

When evaluating threats, vulnerabilities, and potential risks, it's important to monitor multiple sources of information to get a more complete picture of the overall landscape. While CISA ICS Advisories encompass large amounts of data, there are other sources that analysts, asset owners, and security researchers should monitor for vulnerability information.

As an example of the importance of monitoring multiple sources for CVE data, the following is a sample of CVEs reported during the last week of June 2023 with CVSS ratings of "Critical" or "High" from sources outside of CISA advisories.

| CVE | Vendor | Product | CVSS Severity | Link |
|---------------|----------------|-------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2023-2625 | Hitachi Energy | TXpert™ Hub CoreTec™ 4 | Critical | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000163&LanguageCode=en&DocumentPartId=&Action=Launch |
| CVE-2023-0286 | Hitachi Energy | Lumada APM (Asset Performance Management) | High | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch |
| CVE-2023-0215 | Hitachi Energy | Lumada APM (Asset Performance Management) | High | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch |
| CVE-2022-4450 | Hitachi Energy | Lumada APM (Asset Performance Management) | High | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch |
| CVE-2023-0216 | Hitachi Energy | Lumada APM (Asset Performance Management) | High | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch |

| CVE | Vendor | Product | CVSS Severity | Link |
|----------------------|----------------|-------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2023-0217 | Hitachi Energy | Lumada APM (Asset Performance Management) | High | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch |
| CVE-2023-2625 | Hitachi Energy | TXpert™ Hub CoreTec™ 4 | Critical | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000163&LanguageCode=en&DocumentPartId=&Action=Launch |
| CVE-2023-0401 | Hitachi Energy | Lumada APM (Asset Performance Management) | High | https://search.abb.com/library/Download.aspx?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch |
| CVE-2023-1150 | WAGO | Series WAGO 750-3x/-8x products | High | https://cert.vde.com/en/advisories/VDE-2023-005/ |

The ICS Advisory Project provides frequent (often weekly) reports that include both CISA ICS Advisories as well as other CERT and vendor advisories. View previous reports at icsadvisoryproject.com/ics-advisory-summaries.

Organizations tracking CVEs that may be relevant to their environment should be sure to review communications and advisories directly from OEMs and vendors. CVEs are also reported in country CERTs such as Germany (CERT-Bund), Spain (CCN-CERT), Japan (JPCERT), and other open-source resources such as SecurityWizardry.com, and more.

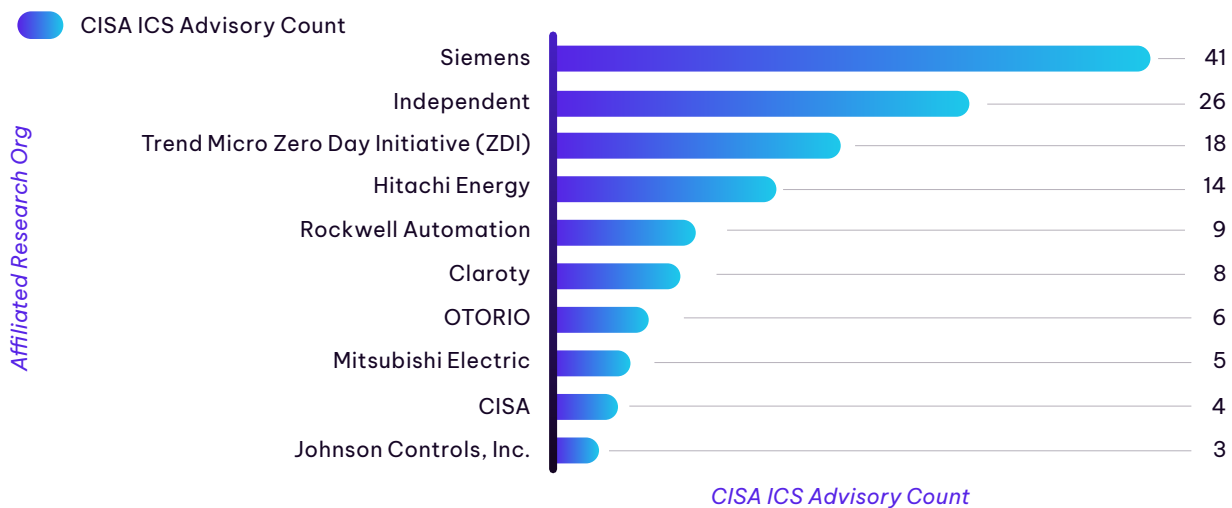


Who is Reporting CVEs?

| Breakout by Reporting Party | 1H23% | 1H22% |
|-----------------------------|-------|--------------------------|
| OEM | 56.1% | 56.4% |
| Security Vendor | 28.5% | 33.9% |
| Independent | 9.4% | 8.4% |
| Academic Research | 3.9% | (not broken out in 1H22) |
| Government | 1.8% | 0.7% |
| Asset Owner | 0.2% | 0.5% |

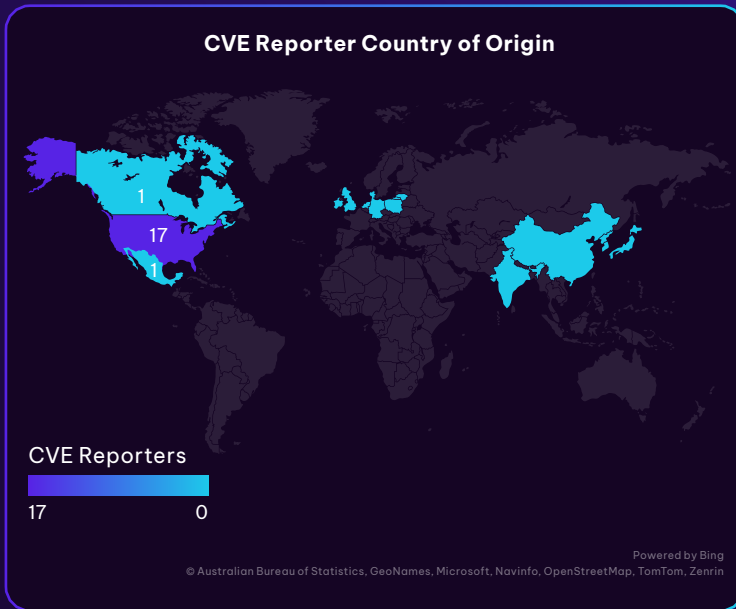
The majority of CVEs reported during the first half of 2023 was done by OEMs and security vendors. This aligns with the trends in CVE reporting throughout the first and second halves of 2022 combined. In 2023, there appears to be more CVE reporting from Academic Research teams than Government and Asset Owners.

CISA ICS Advisory Count by Affiliated Research Org



The ICS[AP] data on the Top 10 Affiliated Research Organizations shows Siemens as the leading OEM producing CVEs through the first half of 2023. They are followed closely by Independent Researchers (in aggregate) and Trend Micro Zero Day Initiative (ZDI) as the top three research organizations.

KEY INSIGHT #2



Looking at reporters by country of origin, a majority of CVE reports originated from OEMs and Security Vendors in the United States, followed by China, Israel, and Japan.

| Country | Independent Researcher Count |
|---------------|------------------------------|
| United States | 7 |
| Unknown | 1 |
| France | 1 |
| Brazil | 1 |
| Germany | 1 |
| Indonesia | 1 |
| India | 1 |
| Israel | 1 |
| Turkey | 1 |
| Lithuania | 1 |
| Total | 16 |

| Country | Count | Percentage |
|----------------|-------|------------|
| United States | 17 | 32.08% |
| Japan | 3 | 5.66% |
| Israel | 3 | 5.66% |
| China | 3 | 5.66% |
| United Kingdom | 2 | 3.77% |
| Taiwan | 2 | 3.77% |
| Switzerland | 2 | 3.77% |
| South Korea | 2 | 3.77% |
| Netherlands | 2 | 3.77% |
| Lithuania | 2 | 3.77% |
| India | 2 | 3.77% |
| Germany | 2 | 3.77% |
| Austria | 2 | 3.77% |
| Worldwide | 1 | 1.89% |
| Poland | 1 | 1.89% |
| Mexico | 1 | 1.89% |
| Macedonia | 1 | 1.89% |
| Ireland | 1 | 1.89% |
| Denmark | 1 | 1.89% |
| Canada | 1 | 1.89% |
| Belgium | 1 | 1.89% |
| Australia | 1 | 1.89% |

The 97 CVEs in the Independent category were reported by 16 individuals. Of the CVE reports from the 16 individual independent researchers, the majority originated from the United States, followed by multiple other countries shown above.

Who is Most Impacted?

| Critical Infrastructure Sector Most Likely to be Impacted by the CISA ICS Advisory | 1H23 CISA ICS Advisory Count <small>(note that some advisories impact multiple sectors)</small> |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Chemical | 7 |
| Commercial Facilities | 11 |
| Communications | 10 |
| Critical Manufacturing | 69 |
| Dams | 2 |
| Energy | 45 |
| Food & Agriculture | 6 |
| Government Facilities | 4 |
| Healthcare & Public Health | 7 |
| Information Technology | 3 |
| Multiple Critical Sectors* | 66 |
| Transportation Systems | 8 |
| Water & Wastewater Systems | 16 |

The critical infrastructure sectors most likely to be impacted by CVEs reported in the first half of 2023 were Manufacturing (37.3% of total reported CVEs) and Energy (24.3% of the total reported).

*CISA ICS Advisories occasionally list “Multiple” under “Critical Sectors Affected” instead of listing affected sectors individually. Any individually listed sector is reflected in its column total above. Multiple Critical Sectors reflects those advisories where sectors were not listed individually.

KEY INSIGHT #3

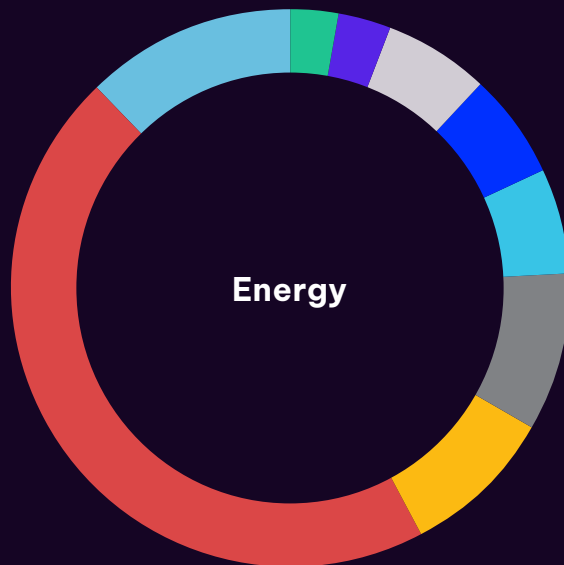
The following pie charts break down the most affected vendor products within the critical infrastructure sectors most likely to be impacted:

| Vendor Products impacted | Percentage |
|--------------------------|------------|
| InHand Networks | 2.3% |
| ABB | 4.5% |
| Schneider Electric | 4.5% |
| Johnson Controls Inc. | 6.8% |
| Advantech | 9.1% |
| Delta Electronics | 11.4% |
| Mitsubishi Electric | 20.5% |
| Siemens | 18.2% |
| Rockwell Automation | 15.9% |



Mitsubishi Electric was the most impacted vendor in the Critical Manufacturing sector (20.5%), followed closely by Siemens (18.2%), and Rockwell Automation (15.9%).

| Vendor Products impacted | Percentage |
|--------------------------|------------|
| Rittal | 2.6% |
| mySCADA Technology | 2.6% |
| Siemens | 5.3% |
| Schneider Electric | 5.3% |
| ABB | 5.3% |
| Rockwell Automation | 7.9% |
| Delta Electronics | 7.9% |
| Hitachi Energy | 39.5% |
| Advantech | 10.5% |



In the Energy sector, Hitachi Energy was the most likely vendor to be impacted by CISA-reported CVEs (39.5%), followed by Advantech (10.5%) as well as Delta Electronics and Rockwell Automation (both 7.9%).

Probability of CVE Exploitation

| Identifying low probability of successful CVE exploitation | 1H23 Count | 1H23% | 1H22 Count | 1H22% |
|------------------------------------------------------------|------------|--------|------------|-------|
| CVEs that require both local/physical AND user interaction | 107 of 670 | 15.97% | 46 of 681 | 6.8% |

When determining the level of risk or prioritization of a CVE in an environment, the probability of successful exploitation for the CVE should be considered. The data above shows that there are a number of CVEs that require both local/physical access AND user interaction for successful exploitation. While these factors do not remove the threat of exploitation, it does decrease its likelihood.

The number of reported CVEs that require both local or physical access AND user/operator interaction have increased with each report, demonstrating the importance of taking vector and probability of exploitation into account, regardless of the total number of CVEs.

| Require User Interaction, regardless of network availability | 1H23 Count | 1H23% | 1H22 Count | 1H22% |
|-------------------------------------------------------------------|------------|-------|------------|-------|
| CVEs that require the user (operator) to take some sort of action | 163 of 670 | 24.3% | 198 of 681 | 29.1% |

The percentage of CVEs that require user action, regardless of network availability, has stayed relatively constant. In the first half of 2022, 29.1% of CVEs required user action. This number has decreased to 24.3% in the first half of 2023.

Understanding CVE Criticality

In addition to the key insights listed previously, SynSaber and ICS[AP] researchers sought to analyze CVE data by criticality, in an effort to understand which CVEs require more immediate attention.

CVEs by CVSS Criticality, First Half of 2023

| | 1H 2023 Count | Percentage of Total (670) | 1H 2022 Count | Percentage of Total (681) |
|-----------------|----------------------|---------------------------|----------------------|---------------------------|
| Critical | 88 | 13.1% | 152 | 22.3% |
| High | 349 | 52.1% | 289 | 42.4% |
| Medium | 215 | 32.1% | 205 | 30.1% |
| Low | 18 | 2.7% | 35 | 5.1% |
| | High/Critical | 65.2% | High/Critical | 64.76% |

| CVSS ATTACK VECTOR | | | | | |
|--------------------|------------------|------------|------------|-----------|-------------|
| CVSS Base Severity | Adjacent_Network | Local | Network | Physical | Grand Total |
| Critical | | | 88 | | 88 |
| High | 7 | 152 | 190 | | 349 |
| Medium | 3 | 105 | 95 | 12 | 215 |
| Low | 1 | 13 | 3 | 1 | 18 |
| Grand Total | 11 | 270 | 376 | 13 | 670 |

Note: All CVEs with “Critical” CVSS Base Severity have a network attack vector.

UNDERSTANDING CVE CRITICALITY

The percentage of reported CVEs with no available patch or remediation reported in the first half of 2023 (34%) has increased substantially when compared to the first half of 2022 (13%). This could be attributed to a number of products that are no longer supported/at end-of-life (see below).

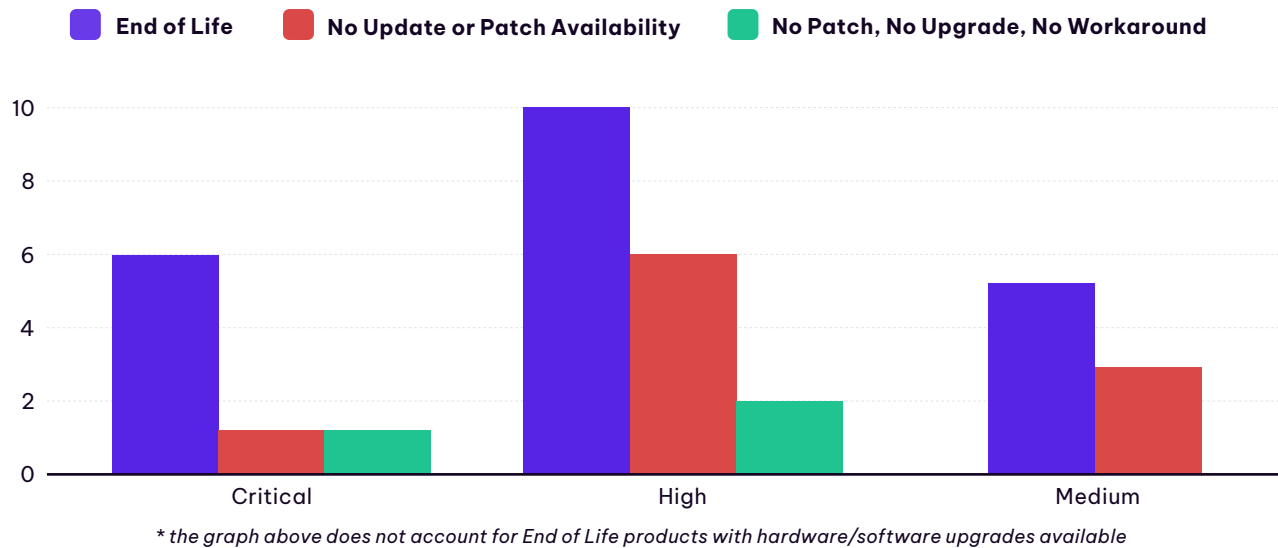
This can also be attributed to the [Siemens advisory](#) mentioned previously with 108 associated CVEs. All 108 vulnerabilities are in the Linux kernel, and there is currently no patch available for these vulnerabilities in the Siemens SIMATIC product.

CVEs with NO Patch or Remediation (“Forever-Days”)

| | 1H23 Count | 1H23% | 1H22 Count | 1H22% |
|-------------------------------------------------------|------------|-------|------------|-------|
| No patch or remediation available at this time | 227 of 670 | 34% | 88 of 681 | 13% |

| Vendor Product End of Life | Severity | Mitigation Status |
|----------------------------------------------------------------|----------|-------------------------------------|
| Akuvox E11 Publication | Critical | No Update or Patch Availability |
| CP-Plus KVMS Pro | High | No Update or Patch Availability |
| RoboDK | High | No Update or Patch Availability |
| ProPump and Controls Osprey Pump Controller | High | No Update or Patch Availability |
| Enphase Installer Toolkit Android App (Update A) | High | No Update or Patch Availability |
| XINJE XD | High | No Update or Patch Availability |
| Nexx Smart Home Device | High | No Update or Patch Availability |
| Atlas Copco Power Focus 6000 | Medium | No Update or Patch Availability |
| SOCOMEK MODULYS GP | Medium | No Update or Patch Availability |
| Enphase Envoy | Medium | No Update or Patch Availability |
| Industrial Control Links ScadaFlex II SCADA Controllers | Critical | No Patch, No Upgrade, No Workaround |
| Panasonic Sanyo CCTV Network Camera | High | No Patch, No Upgrade, No Workaround |
| Carlo Gavazzi Powersoft | High | No Patch, No Upgrade, No Workaround |

Forever-Day Vulnerabilities by Severity

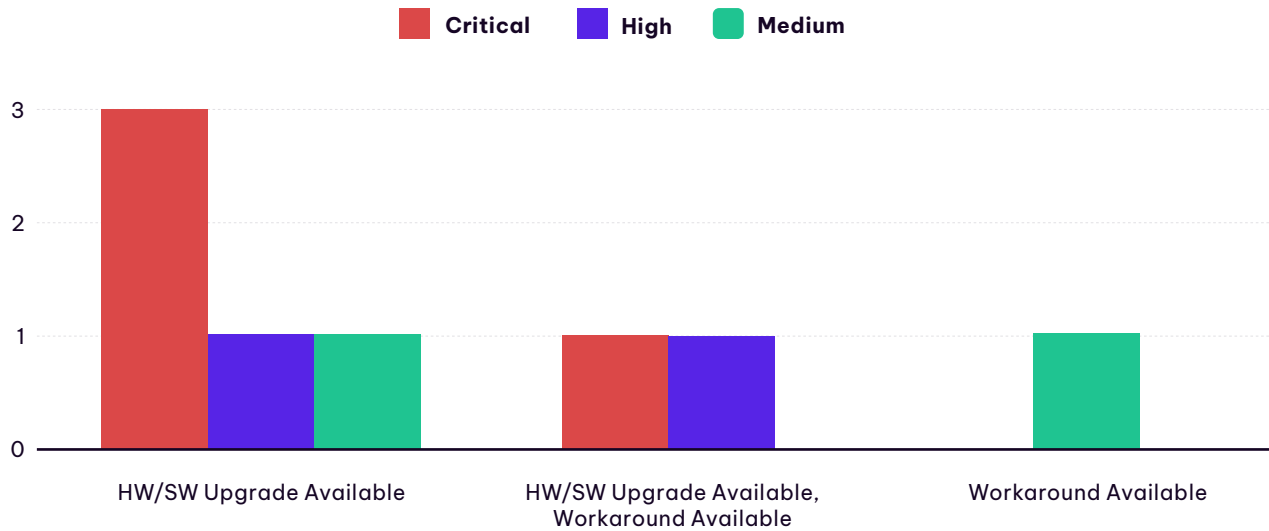


In reviewing “critical” and “high” severity levels, there were six CISA Advisories identified for ICS vendor products that reached end of life with “critical” severity vulnerabilities that have no update, patch, hardware/software/firmware updates, or known workarounds.

There were ten CISA advisories for ICS vendor products that reached end of life with “high” severity levels. Six of these ten had no update or patch available. Two of these ten had no patch, upgrade, or workaround.

| Vendor Product End of Life | Severity | Mitigation Status |
|-------------------------------------------------------------|----------|-----------------------------------------------|
| Rockwell Automation products using GoAhead Web Server | Critical | HW/SW Upgrade Available |
| Keysight N8844A Data Analytics Web Service | Critical | HW/SW Upgrade Available |
| SAUTER Controls Nova 200 - 220 Series (PLC 6) | Critical | HW/SW Upgrade Available |
| Siemens SIMATIC STEP 7 and Derived Products | Critical | HW/SW Upgrade Available, Workaround Available |
| Siemens in OPC Foundation Local Discovery Server | High | HW/SW Upgrade Available, Workaround Available |
| Hitachi Energy’s AFS65x, AFS67x, AFR67x and AFF66x Products | High | HW/SW Upgrade Available |
| Rittal CMC III Access systems | Medium | Workaround Available |
| Hitachi Energy FOXMAN-UN and UNEM Products | Medium | HW/SW Upgrade Available |

Products with Forever-Day Vulnerabilities & Mitigation Options by Severity



In the first half of CISA-reported ICS Advisories for 2023, there were eight vendors for products with options for asset owners to migrate to new hardware/software/firmware or implement a workaround for the forever-day vulnerability.

Three vendor products with “critical” forever-day vulnerabilities have only the option to migrate to updated hardware/software, and one product has the option of an update or implementing a workaround.

Two “high” severity forever-day vulnerabilities offer either a hardware/software upgrade or available workaround.

Most Dangerous Software Weaknesses (MDSW)

On June 29, 2023, CISA announced the Homeland Security Systems Engineering and Development Institute, sponsored by the Department of Homeland Security and operated by MITRE, and has released the [2023 Common Weakness Enumeration \(CWE\) Top 25 Most Dangerous Software Weaknesses](#).

Analyzing the first half of CISA-reported ICS Advisories in 2023, the following Top 5 MDSW were associated with ICS CVEs:

Top 5 Most Dangerous Software Weaknesses Associated with CISA ICS Advisory CVEs

CWE-416: Use After Free














CWE-125: Out-of-bounds Read

CWE-20: Improper Input Validation

CWE-787: Out-of-bounds Write

CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’)

UNDERSTANDING CVE CRITICALITY

| | Percentage |
|----------------------------------------------------------------------------------------------------------|------------|
|  Sewio | 2.5% |
|  Delta Electronics | 5.0% |
|  Sub-IoT project | 2.5% |
|  Autodesk | 2.5% |
|  Schneider Electric | 2.5% |
|  Nexx | 2.5% |
|  JTEKT ELECTRONICS C... | 5.0% |
|  Datakit | 2.5% |
|  Snap One | 2.5% |
|  Hitachi Energy | 10.0% |
|  Horner Automation | 5.0% |
|  Rockwell Automation | 10.0% |
|  Siemens | 47.5% |



These Top 5 MDSW affected Siemens products the most, followed by Rockwell Automation and Hitachi Energy products. CISA has stated these weaknesses can lead to serious vulnerabilities in software. An attacker can often exploit these vulnerabilities to take control of an affected system, steal data, or prevent applications from working.

Asset owners and operators should review the [CWE Top 25](#) or view the ICS Advisory Project COMMON WEAKNESS ENUMERATION (CWE) VIEW Dashboard to identify affected products used in their OT environments.

These CWEs can not be directly remediated by operators. Instead, operators should evaluate and consider what mitigations are most suitable for their operational environment. If no suitable mitigation is available, consult with the vendor of the affected product about potential workarounds.

We provide this information to empower those involved with the remediation of vulnerabilities in an ICS environment to discuss these common software weaknesses with OEMs.

Prioritizing and Taking Action on CVEs

When reviewing the CVEs and determining which should be addressed in your environment, there are several factors to consider that will help in determining relevance and urgency of remediation or mitigation

Vulnerabilities listed in the KEV (Known Exploited Vulnerabilities) catalog published by CISA indicate that there are or have been active, observed attempts at exploiting the vulnerability, and should be prioritized accordingly. Any assets impacted by CWEs (Common Weakness Enumeration) in the MDSW (Most Dangerous Software Weaknesses) list should also be prioritized.

The EPSS score (Exploit Prediction Scoring System) and CVSS (Common Vulnerability Scoring System) should be consulted, as these score the likelihood of the vulnerability's exploitation.

What is CVSS? CVSS is a standardized methodology for assessing and communicating characteristics of software vulnerabilities. It helps us to prioritize and understand risks. CVSS has three main components: Base, Temporal, and Environmental metrics. Base metrics evaluate inherent vulnerability characteristics. Temporal metrics consider time-dependent factors. Environmental metrics account for the specific organizational context.

The CISA ICS Advisories and the National Vulnerability Database (NVD) only report Base metrics for CVEs, and it is left to the operator to evaluate Temporal and Environmental metrics if they so choose.

The CVSS score may range from 0.0 to 10.0 and is calculated solely from the values of its components. Knowing the individual values which make up the CVSS vector for a CVE can provide context beyond the CVSS score itself. Knowing that the CVSS score is 9.4 provides little actionable information, but knowing that the Attack Vector is Network and the Privileges Required are High could give an operator a starting point for evaluating the security of the system.

CVSS scores may be higher or lower than the published value in your specific environment. Utilizing the components of CVSS combined with knowledge of your environments will allow you to assess the risk and priority in your organization.

While CVSS doesn't apply perfectly to industrial control environments, it can be used as a prioritization method and framework across different vulnerabilities. CVEs are scored 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)

The attack vector and complexity should also be taken into account with each vulnerability to determine the context and relevance to your own environment.

When evaluating a CVE's relevance to your environment, consider these questions:

- Is the potentially affected network segmented?
 - ▷ Does this network sit behind a firewall?
- Are these environments' networks and/or systems monitored?
- Is this environment accessible remotely?
 - ▷ If so, how is this achieved? Is a jump host or VPN utilized?
 - How is access managed and authenticated, and is it monitored?
- What are the physical security controls and considerations you have in place?
- Is this asset(s)/device(s) currently supported?
 - Is this environment under a maintenance contract?
 - ▷ What are the vendor/OEM's policies?
- How is the device configured? Is the cited vulnerability relevant in this configuration? (Is the component enabled?)
- What security controls do you have in place, and how might they mitigate or be used to mitigate any risk posed?

When assessing the relevance of vulnerabilities to your environment, it may be helpful to group them into vulnerabilities that need to be addressed immediately, those that should be addressed in the future, and those where addressing them will take significantly more effort.



NOW

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



NEXT

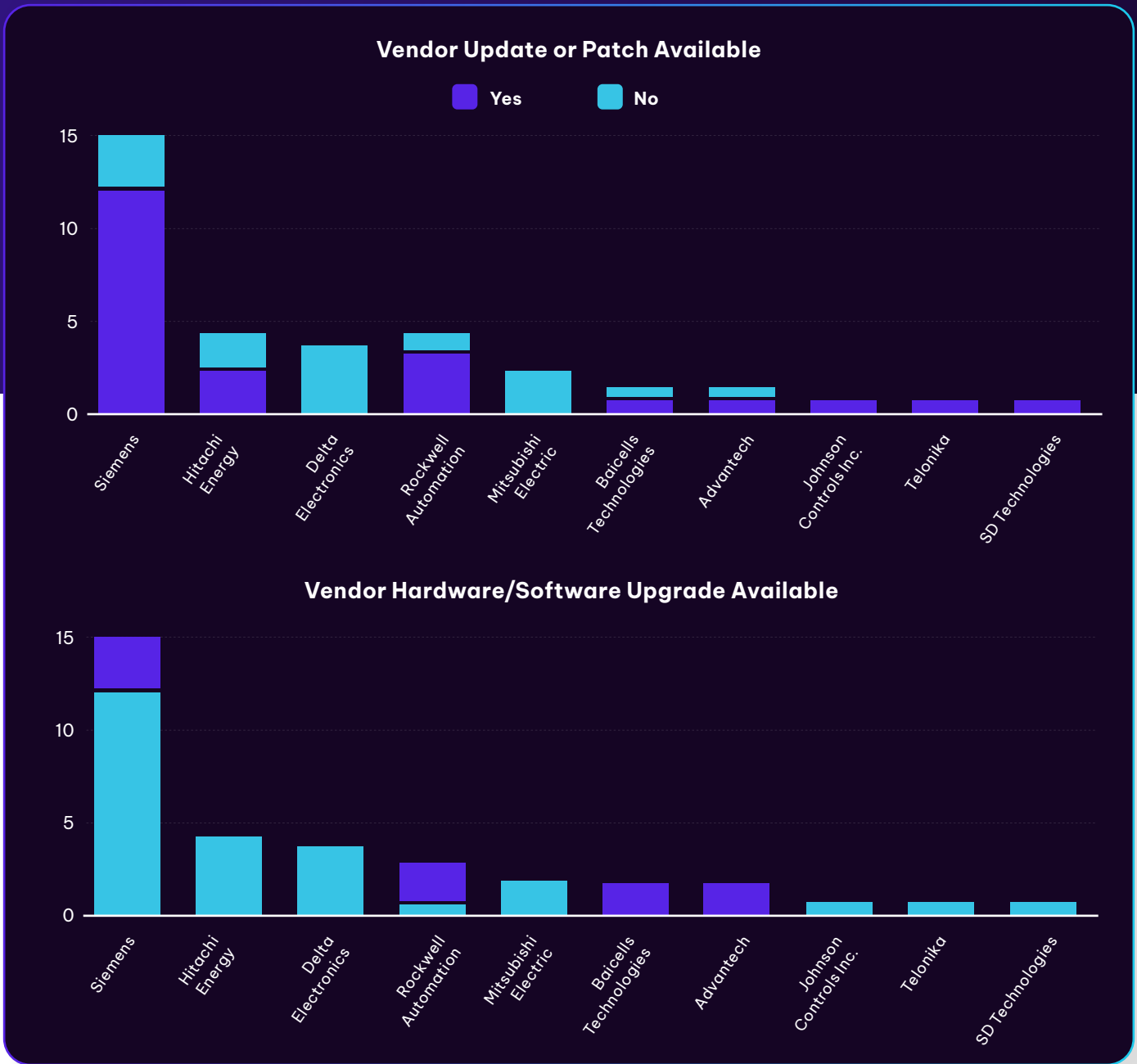
These CVEs are more complex from a remediation perspective but still require attention. Examples include firmware updates that could affect a large number of fielded devices.



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.

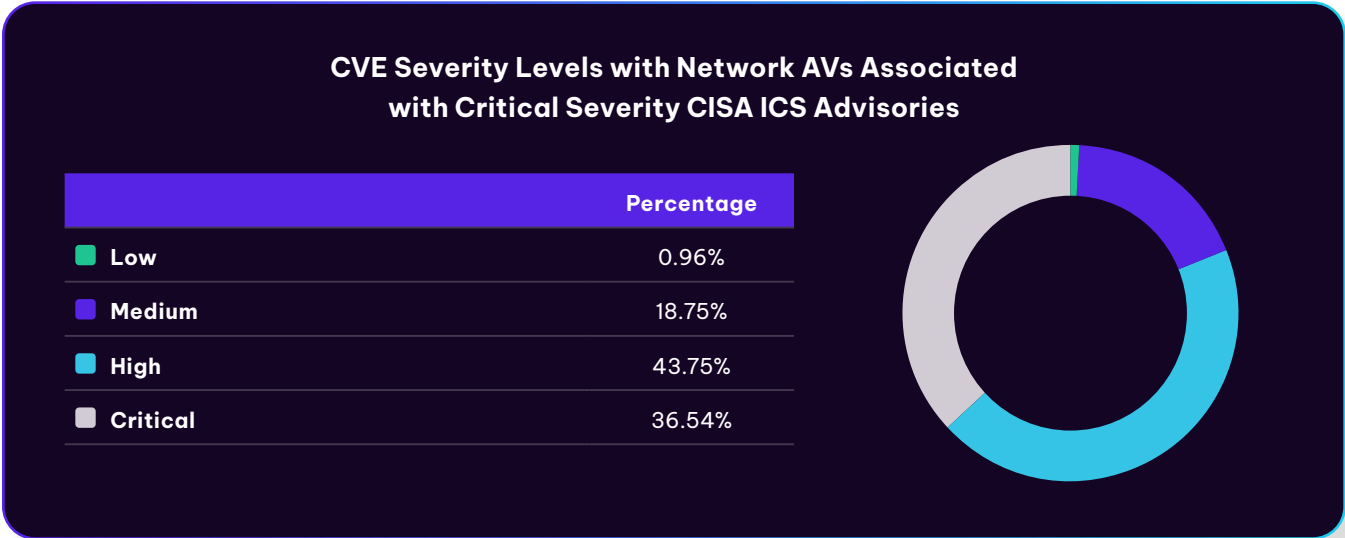
Prioritization Example & Walkthrough



Out of the 53 “critical” severity vulnerabilities with available updates, patches, and/or hardware/software upgrades, Siemens and Hitachi Energy had the most CISA ICS Advisories. Organizations with large numbers of Siemens and Hitachi Energy products should review these vulnerabilities to determine the feasibility of applying the available patches, or consider the option to migrate to the next hardware/software version available to mitigate these vulnerabilities.

None of the 53 “critical” severity vulnerabilities identified in new CISA ICS Advisories were flagged for correlation to the CISA KEV catalog CVEs, which should be considered when prioritizing critical severity mitigation.

There are also other factors to consider in prioritizing the mitigation of critical severity vulnerabilities, including the CVSS vector data for each CVE. For example, CVEs with “NETWORK” Attack Vectors (AV) should be considered a higher priority over “LOCAL” AVs.



There were 208 CVEs associated with critical severity CISA ICS Advisories that had NETWORK AVs. While the CISA ICS Advisories were identified as critical, the CVE’s severity associated with the advisories may be lower. There are 36.54% “critical” severity level CVEs, 43.75% “high” severity, and the remaining ~20% are “medium” or “low” severity level CVEs.

An asset owner or operator can focus on addressing the “critical” severity CVEs with Exploitation Predictability Scoring System (EPSS) scores of 90th percentile or higher to prioritize mitigations in absence of CVEs being flagged in the CISA KEV catalog.

| CVE | CVSSv3 Score | CVSSv3 Severity | CVSSv3 Vector | EPSS | PERCENTILE |
|----------------------|--------------|-----------------|-------------------------------------|------|------------|
| CVE-2022-1292 | 9.8 | Critical | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 0.45 | 96.88% |
| CVE-2023-1133 | 9.8 | Critical | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 0.08 | 93.49% |
| CVE-2019-5096 | 9.8 | Critical | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 0.39 | 96.72% |
| CVE-2021-3711 | 9.8 | Critical | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 0.05 | 91.84% |
| CVE-2022-2068 | 9.8 | Critical | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 0.18 | 95.44% |

Drilling down on the five critical CVEs with EPSS scores at 90% or above with NETWORK AVs (shown above), it becomes easier to focus on prioritizing mitigation planning instead of focusing on addressing 208 individual CVEs with critical severity levels.

An asset owner or operator can look at how many CVEs impact multiple CISA ICS Advisories. CVE-2022-1292, for example, affects five Siemens products alone.

| Alert Code | Date | Vendor | Product | Cumulative CVSS | Severity | CVEs |
|----------------|-----------|---------------------|----------------------------------------------------------|-----------------|----------|--------------------------------|
| ICSA-23-166-11 | 15-Jun-23 | Siemens | SIMATIC S7-1500 TM MFP | 9.8 | Critical | CVE-2022-1292 |
| ICSA-23-166-12 | 15-Jun-23 | Siemens | SINAMICS MV (medium voltage) products | 9.8 | Critical | CVE-2022-1292 |
| ICSA-23-075-01 | 16-Mar-23 | Siemens | Busybox Applet affecting SCALANCE and RUGGEDCOM products | 9.8 | Critical | CVE-2022-1292 |
| ICSA-23-047-03 | 16-Feb-23 | Siemens | Brownfield Connectivity Client | 9.8 | Critical | CVE-2022-1292 |
| ICSA-23-017-03 | 17-Jan-23 | Siemens | SINEC INS | 9.9 | Critical | CVE-2022-2068 CVE-2022-1292 |
| ICSA-23-143-02 | 23-May-23 | Hitachi Energy | RTU500 Series | 9.8 | Critical | CVE-2021-3711 |
| ICSA-23-026-06 | 26-Jan-23 | Rockwell Automation | Products using GoAhead Web Server | 9.8 | Critical | CVE-2019-5096 |
| ICSA-23-080-02 | 21-Mar-23 | Delta Electronics | InfraSuite Device Master | 9.8 | Critical | CVE-2023-1133 |

Environments with these products in their OT environments with remote access might present an easy target. Critical severity CISA ICS Advisories with NETWORK AVs and high EPSS scores should be a high priority for an organization's plan of action or a key milestone in mitigation efforts if you can't ensure that these systems are completely isolated from remote access, or secure remote access isn't guaranteed.

Not Every Patch Is Associated with a CVE!

CISA Advisories can contain multiple CVEs. It's not uncommon for a vendor or OEM to release a security patch without a CVE attached to it.

An example of this can be seen with [AVEVA InTouch Access Anywhere and Plant SCADA Access Anywhere](#). AVEVA published a security bulletin detailing the vulnerability, recommendations, and the available [security update downloads](#).

There are three distinct CVEs associated with the CISA advisory ([CVE-2020-11022](#); [CVE-2021-3711](#); [CVE-2022-23854](#)), but only one of them (CVE-2022-23854) lists AVEVA with the CVE's CPEs. The other two CVEs do affect AVEVA devices, but because the underlying vulnerabilities are in jQuery (CVE-2020-11022) and OpenSSL (CVE-2021-3711), AVEVA is not issued its own CVEs per MITRE guidelines.

In Conclusion



As previously witnessed, the number of CVEs reported via CISA ICS Advisories and other alerting groups is likely to continue increasing over time or at least remain relatively steady. Understanding which CVEs are “forever-day vulnerabilities” will reduce the number of vulnerabilities that need to be accounted for in a vulnerability remediation plan.

Effective prioritization of both CVEs and other vulnerabilities leverages both CISA ICS Advisories as well as other officially sanctioned and community-driven resources. Care should be taken to understand vulnerabilities in the context of the environments in which they appear. Since every OT environment is unique and purpose-built, the likelihood of exploitation and impact that it may have will vary greatly for each organization.

SynSaber and the ICS Advisory Project will continue monitoring and analyzing reported CVEs and will provide updated reports as new trends and findings emerge over time.



SYNSABER

ICS[AP]

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. You can learn more about the ICS Advisory Project by contacting icsadvisorypro@icsadvisoryproject.com or by visiting icsadvisoryproject.com

RESEARCH SCOPE

- For consistency, metrics in this report are limited to CVEs as reported by CISA ICS Advisories.
- The time period for this data runs from 1 January 2023 – 30 June 2023, except as indicated for comparative analysis.
- Note that CISA continually updates ICS Advisories as required, so specific metrics may vary slightly after report publication.
- The 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, the affected vendor, or the NVD.
- When the terms “reported CVEs,” “CVEs reported to CISA,” “groups reporting CVEs,” etc. are used, we mean that those CVEs were submitted to CISA as being present in an ICS device or software and were published in a CISA ICS Advisory. Note that a CISA advisory may not be the first appearance of a CVE, and that the party who reported the CVE to CISA may not be the original discoverer of the vulnerability. All reporter statistics are calculated solely from ICS Advisories and represent the parties reporting to CISA.

TERMS, DEFINITIONS, AND NOTES

CISA

The Cybersecurity and Infrastructure Security Agency is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

CPE

The Common Platform Enumeration is a structured naming scheme for information technology systems, software, and packages. The structure and dictionary is maintained by NIST (National Institute of Standards and Technology).

CVE

Common Vulnerabilities and Exposures. This system classifies vulnerabilities and assigns them an ID number for reference.

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.

CWE

Common Weakness Enumeration is a community-developed list of common software and hardware weakness types.

EPSS

The Exploit Prediction Scoring System provides a score that estimates the likelihood that a vulnerability will be exploited. The higher the score, the greater the probability that a vulnerability will be exploited.

ICS

Industrial Control System, also referred to as Operational Technology (OT) systems, Supervisory Control and Data Acquisition (SCADA) or Cyber-Physical systems. These systems focus on industrial processes and automation rather than traditional enterprise or information technology (IT) environments.

TERMS, DEFINITIONS, AND NOTES

KEV

The [Known Exploited Vulnerabilities catalog](#) is a source of vulnerabilities that have been exploited in the wild. Vulnerabilities in the KEV catalog are CVEs that are actively being exploited, were previously exploited, or there were attempts at exploitation.

MDSW

The Most Dangerous Software Weaknesses was calculated analyzing public vulnerability data in the US National Vulnerability Database (NVD) for root causes via CWE mappings.

MITRE

The MITRE Corporation is a non-profit organization and federally-funded R&D center (FFRDC) working in conjunction with CISA and NIST and is the owner of the CVE project.

NIST

National Institute of Standards and Technology.

NVD

The National Vulnerability Database is the US government repository for vulnerability data, including CVEs, CPEs, CVSS scores, and CWEs.

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.

Other: The vulnerability affects a device or application which has no patch at time of publication or which is end-of-life. Other measures must be taken to avoid exploitation, including but not limited to: system upgrades, additional monitoring, disabling of certain device functions, or physical security measures.

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 user interaction with the system (Local) or direct physical access to the device (Physical).

ADDITIONAL RESOURCES

SynSaber Resources

[Webinar: March 2023 - Analyzing 3 years of ICS Advisories](#)

[Webinar July 2023 - First Half of 2023 ICS CVE stats](#)

[Previous ICS CVE Reports](#)

[OT PCAP Analyzer Free Community Tool](#)

ICS Advisory Project Resources

[ICS Advisory Project Dashboards](#)

[ICS Advisory Project GitHub](#)

Other Resources

[MITRE ATT&CK ICS Techniques](#)

[Free online & in-person ICS security training via CISA](#)

[How to Calculate Cyber Attack Likelihood Using Exploitability Assessment](#)

CONTRIBUTORS

Daniel Ricci | Kylie McClanahan | Jori VanAntwerp | Celyn Matienzo

ABOUT SYNSABER

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. SynSaber is privately held with funding from SYN Ventures, Rally Ventures, and Cyber Mentor Fund. Learn more at [SynSaber.com](#).

info@synsaber.com

Follow SynSaber on social media

[Twitter](#), [LinkedIn](#), [YouTube](#)

ABOUT ICS ADVISORY PROJECT

The ICS Advisory Project is an open-source analysis tool for OT asset owners, CISOs, cybersecurity analysts, and researchers to identify threats and vulnerabilities by product, vendor, and critical infrastructure sector. The project's interactive dashboards are the result of countless hours of research, analysis, and data enrichment by founder Dan

Ricci and community volunteers using CISA ICS Advisories, CVEs, MITRE ATT&CK, and other threat/vulnerability data. The full ICS[AP] dataset is publicly available via a GitHub Repository. Learn more at [ICSAdvisoryProject.com](#).

icsadvisorypro@icsadvisoryproject.com

Follow ICS[AP] on social media

[Twitter](#), [Discord](#), [LinkedIn](#)



SYNSABER ICS[AP]