INDUSTRIAL VULNERABILITY SCORING STUDY

A STUDY OF THE COMMON VULNERABILITY SCORING SYSTEM (CVSS), ITS VIABILITY IN ICS/OT, AND POTENTIAL ALTERNATIVE SOLUTIONS

LOGIIC™ ThreatGEN

Revision	Date
First Draft	11/17/2022
Final Draft	3/31/2022

This study and report were produced by ThreatGEN via contract paid for by LOGIIC.

2 Overview

The purpose of this study is to evaluate the Common Vulnerability Scoring System (CVSS)[1] effectiveness and applicability to industrial vulnerabilities, consequences, and impacts to industrial processes. It aims to determine the need, and/or the industrial community's desire, for supplemental or alternative vulnerability scoring methods, which could be better suited for industrial environments (ICS/OT). Additionally, it will suggest potential changes to the CVSS, or a separate augmentative solution, which could be better suited for industrial systems.

2.1 What is the CVSS

The CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities. Owned and managed by FIRST.Org, Inc. (FIRST)[2], it has been in use as an industry standard since 2007, when version 2 was released[3]. The CVSS is currently in version 3.1 and is continually supported and updated through the efforts of the CVSS-SIG (special interest groups)[4].

The CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. The most current version of the CVSS calculator[5] version 3.1, but version 2 is still in use by the National Vulnerability Database[6]. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score, as specified in the official documentation[7].

2.2 CVSS Criticism from the Industrial (ICS/OT) Community

A common criticism[8] of the CVSS (throughout the broader cybersecurity community and not just ICS/OT) is that it does not intuitively address vulnerability scores in the context of overall risk. The inclusion of variables pertaining to the impact to data confidentiality, integrity, and availability (CIA) infers an application to risk, but the (supplemental) environmental metrics (which must be adjusted by the end-user and is required to make each CVSS score relevant to your risk profile) can be vague and confusing. Furthermore, a majority of end-users do not adjust the environmental metrics (discussed

[1] https://www.first.org/cvss/
[2] https://www.first.org/about/
[3] https://www.first.org/cvss/v2/history
[4] https://www.first.org/global/sigs/
[5] https://www.first.org/cvss/calculator/3.1
[6] https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
[7] https://www.first.org/cvss/v3.1/specification-document
[8] https://www.redhat.com/en/blog/why-cvss-does-not-equal-risk-how-think-about-risk-your-environment

later in this study), which can lead to a misleading CVSS score (as it relates to the context of a specific environment). This is especially problematic when the base CVSS score alone is used as a "risk" score.

Additional criticism is also growing throughout the ICS/OT cybersecurity community, specifically around the CVSS' consideration, or lack thereof, for industrial systems and environments[9][10]. In 2018, Dale Peterson released a special call for presentations for the S4x19 ICS cybersecurity conference[11] to address these concerns and present potential solutions. Art Manion, Billy Rios, and Clint Bodungen each presented 3 different solutions as S4x19. The video recording of their presentations can be found S4 Events' YouTube channel[12]. The overarching concern throughout the ICS/OT cybersecurity community is that the CVSS' focus on the CIA model is geared toward impacts to information security and does not account for cyber-physical consequences and impacts. This leaves industrial operators unable to accurately prioritize the remediation of industrial vulnerabilities. Given the criticality of ICS/OT environments, this is a serious concern.

(NOTE: There is an industrial control system (ISC) SIG within FIRST, but it is currently only designated as a discussion group. The improvements from version 1 through version 3.1 don't seem to have direct consideration for ICS, and the same appears to be true for the release of version 4.0, according to the publicly released list of potential changes[13].)

3 Study Process

In June of 2021, LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity)[14] and ThreatGEN[15], an industrial security firm specializing in industrial cyber risk management, began a joint study to determine the potential need for an alternative vulnerability scoring system for industrial systems, what the requirements would be, and what potential solutions could look like. The study took place between June 2021 and November 2021 and consisted of solution presentations and workshops with LOGIIC members as well as extensive interviews with members of the industrial community.

Industry sectors represented in the interviews were:

- Oil & Gas (upstream, downstream, and midstream)
- Electric Utility (generation, transmission, and distribution)
- Water/Wastewater Utility
- Manufacturing (food & beverage, pharmaceutical, and automotive)

(NOTE: Additional industrial sectors such as healthcare, transportation, etc. were not excluded, but were underrepresented due to lack of response. The results of this study could possibly be refined with the inclusion of other industrial sectors such as these.)

[9] https://www.securityweek.com/cvss-scores-often-misleading-ics-vulnerabilities-experts
[10] https://verveindustrial.com/resources/blog/cvss-scores-is-it-effective-for-ics-vulnerabilities-in-ot/
[11] https://s4xevents.com/
[12] https://www.youtube.com/watch?v=-6cThOCm9co
[13] https://docs.google.com/document/d/1qmmk9TQulW9d1cuipu_ziXDX0pUswbZ1WSQyynHbvKU/edit
[14] https://www.logiic.org/
[15] https://threatgen.com/

To ensure the relevancy and validity of the participants and their responses, participants were qualified and selected based on the following criteria:

Participants must,

- Work in an industrial sector
- Be actively involved with operational (ICS/OT) cyber risk management
- Currently use CVSS or have significant experience using CVSS

(For privacy and security reasons, the names of the participants and the company they work for will not be released in this report.)

Interviews were conducted using a questionnaire either via live conversations over Zoom or Microsoft Teams meetings or by answering the questionnaire via email. The following questions were asked as a basis for the questionnaire as well as to promote more in-depth discussion during live conversations.

1. What industrial sector do you work in?
2. What is the size of your vulnerability management team?
3. Do you currently use CVSS scores in your risk scoring/prioritization?
4. Do you adjust the CVSS environment modifiers in the calculator tool?
5. Do you feel that CVSS adequately represents ICS/OT?
    a. If not, would you use a secondary/supplemental tool to augment/modify the existing base CVSS score to better represent industrial consequences and impact?
    b. Would you prefer a more industry focused option be implemented directly in the CVSS calculator rather than using a separate tool?
6. Would you prefer a vulnerability scoring tool (CVSS or otherwise) with more risk-based metrics?
7. Would you adjust the CVSS environment modifiers in the calculator tool if more risk-based metrics were included?
8. Would you use a separate vulnerability scoring tool (most likely one that still takes into account the base CVSS score), either in conjunction with CVSS or as a complete alternative, if it included more comprehensive risk scoring metrics?
9. What risk-based metrics/variables would you prefer to see in a risk-based vulnerability scoring tool?

Clarification notes were given in the questionnaire document, and participants were allowed to ask for additional clarification if needed.

Throughout this study, a tool currently labeled as the "Industrial Vulnerability Scoring System (IVSS)[16] was used to illustrate potential changes, suggestions, and augmentative industrial metrics to the CVSS. It was actively revised, based on feedback from LOGIIC and the participants.

[16] https://threatgen.com/resources/ivss/

3.1 The Industrial Vulnerability Scoring System (IVSS)

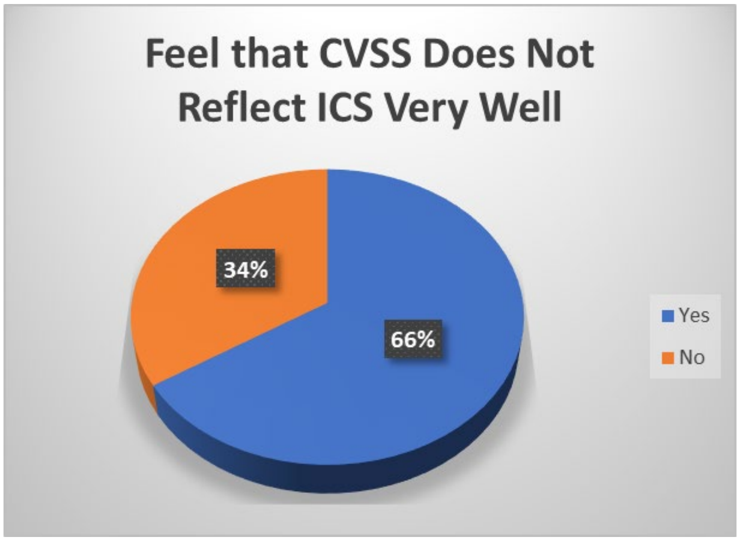
The IVSS is a non-profit, open-source derivative of the CVSS, developed, and currently maintained, by ThreatGEN. The IVSS, however, is designed specifically for industrial control systems vulnerabilities. The IVSS is not meant to be a replacement for the CVSS, but rather an industrialized alternative in terms of the environment modifiers. The goal of the IVSS is to create a conceptual working model of a vulnerability scoring system for ICS/OT, using metrics specific to industrial systems and environments.

While the IVSS base score and the CVSS base score use very similar parameters, the environmental modifiers are where the more industrial focused parameters are considered. Just like the CVSS temporal and environment modifiers, the IVSS ICS environment modifiers are meant to be adjusted by, or with the assistance of, someone who has knowledge of the local environment for the system in question. Due to the common cross-industry acceptance and use of the CVSS, part of the design, currently in process, for the IVSS will be added functionality to reference and use the base CVSS score from existing Common Vulnerability and Exposures (CVE) entries. This will then allow industrial operators to modify the CVSS score using the IVSS local ICS environment modifiers.

The intent of the IVSS is to provide a prototype, which inspires FIRST to integrate ICS/OT metrics into CVSS but is also currently available for public use. The IVSS is still in the early stages of development (alpha) and will continue to be updated and documented as progress is made. The current IVSS specifications and calculations can be found in Appendix A of this report.

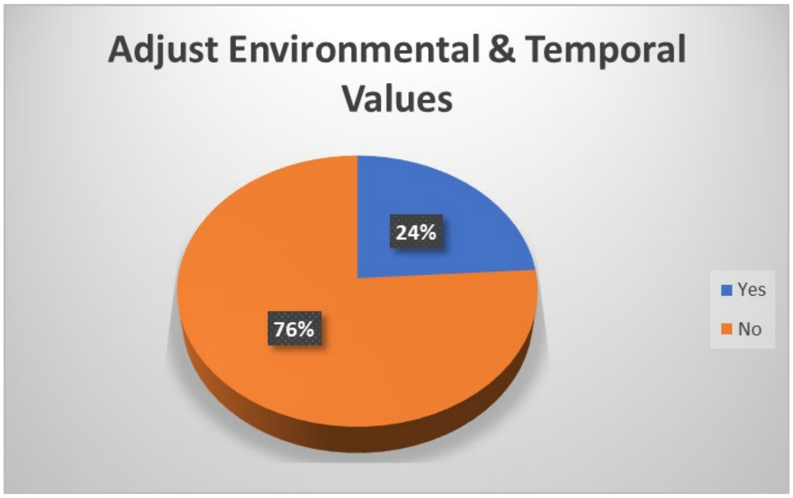
4 Study Results

66% of the study participants felt like the current CVSS does not effectively represent the consequences and impact that successfully exploited vulnerabilities could have on ICS/OT. When considering the CIA model used by the CVSS, participants universally agreed that data and system availability, as well as data integrity, are absolutely paramount in ICS/OT. Data confidentially was generally viewed as a much lower priority, if considered at all. Overall, the consensus was that the CIA-based metrics and calculations, as used in the CVSS, are focused on an information protection context, and not necessarily on data and system consequences and impact. This results in effectively "retrofitting" information protection concepts into ICS/OT context.



Interestingly, while the other 34% of participants agree that the CVSS could be improved to better reflect ICS/OT, they felt that the CIA prioritization metrics do provide enough adjustment to suit their needs, because ICS/OT context can be inferred from the *availability* and *integrity* metrics of the CIA model. The counterargument is that the CIA prioritization then becomes impractical because all ICS/OT scoring would essentially use the same CIA prioritization.

The adjustable environmental metrics were also viewed as vague and having little to no specific relevance to ICS/OT. However, 76% of the participants said that they do not adjust the supplemental temporal and environment metrics sections, mostly due to the level of effort required. Manually adjusting these metrics for hundreds, or even thousands, of vulnerabilities is a daunting task, especially when the relevance to ICS/OT is unclear.



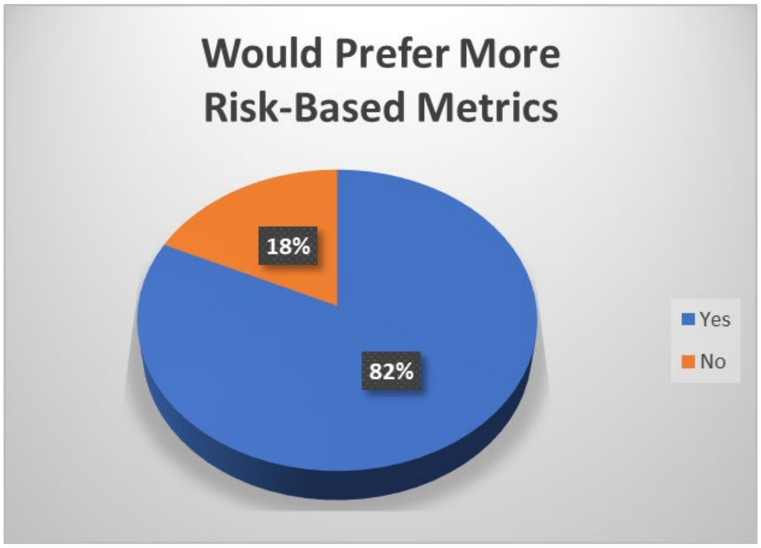
(NOTE: Team size was not considered at the time of this study, with regards to the number of participants who adjust the temporal and environmental values. This metric was pointed out during one of the LOGIIC workshops as being of potential value to the outcomes and conclusions of the study. We are attempting to gather this information from the participants and will revise this report if/when the data is available.)

Regardless of specific environmental relevance (IT vs. ICS/OT), this is a much broader concern when considering CVSS scores for risk prioritization.

The base CVSS score is a general severity rating, which is scored using metrics that are specific only to that vulnerability (e.g., exploit complexity, user interaction and privileges required, etc.), and from a generic perspective. Local environment metrics are, understandably, not considered at the time of initial scoring. When considering CVSS scores as part of an overall risk prioritization strategy, impacts to the local environment should be included. Otherwise, the prioritization could end up being extremely inefficient and inaccurate, due to vulnerability ratings that do not accurately reflect the actual risk to the local environment. This is the intent of the CVSS environmental metrics and can only be adjusted by someone with knowledge of the local environment, since every organization and environment are unique.

The CVSS is intended to be used as a vulnerability scoring tool, which is only one part of an overall risk score. However, many end-users use the CVSS score as a “risk score”. Therefore, the CVSS has evolved to support such usage by adding and increasing more risk relevant metrics (e.g., the temporal and environmental metrics), which end-users can adjust.

That said, a vast majority of participants (82%) would still prefer more risk-based metrics included in the CVSS, beyond what is currently included in the environmental metrics.

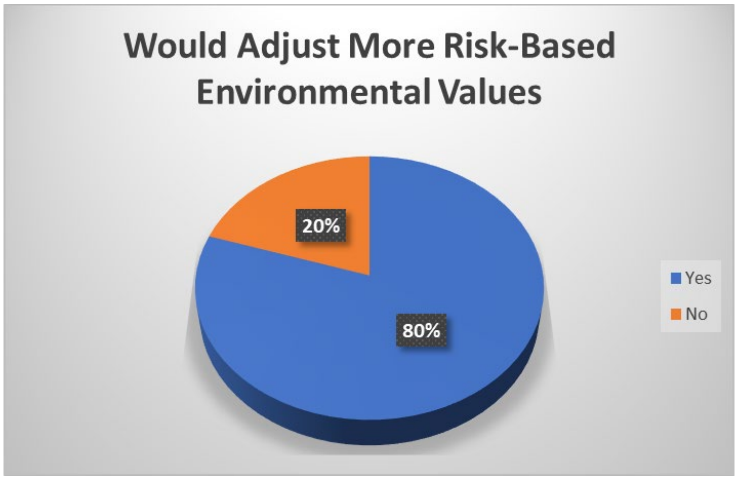


Additional risk-based metrics participants would like to see included are as follows:

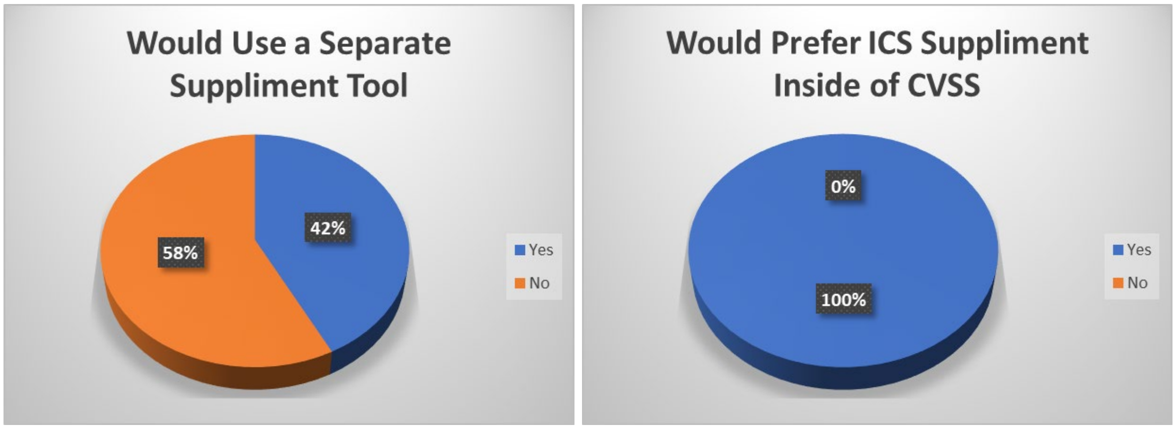
- Financial impact
- Health, Safety, and Environment (HSE) impact
- Network segment/zone location
- Accessibility through the firewall
- Patch frequency
- Compensating controls
- Impacts from the Internet of Things (IoT)
- Loss of visibility, monitoring, and control of the process
- Impact to production and the reliability of the process

The number of participants that said they would complete the environmental values section increased from 24% to 80%, if more risk-based metrics were included.

(NOTE: Again, this is without regard to team size.)



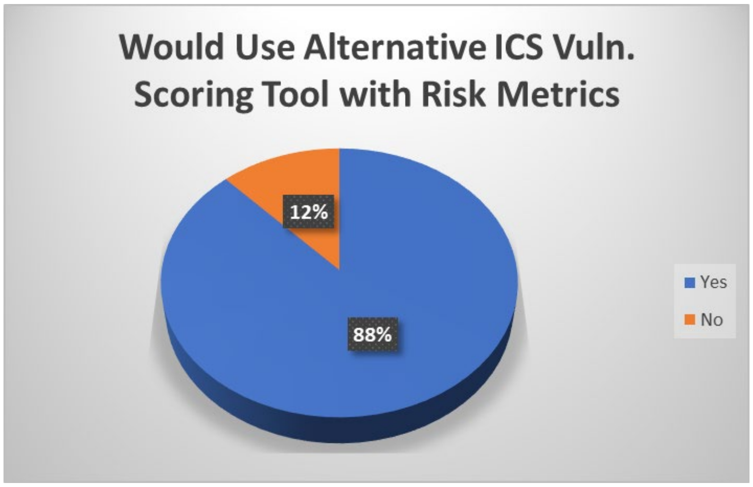
Slightly more than half of the participants (58%) said they would use a completely separate tool to supplement the CVSS with ICS/OT metrics. However, 100% of the participants said they would prefer to have ICS/OT metrics available directly with the CVSS.



Another interesting observation that was not reflected in the questionnaire but was discussed in live conversations was whether the supplemental tool should use the exact same base score as the CVSS. Many participants had little to no preference whether the ICS/OT metrics were included in the CVSS or in a separate tool. This was largely due to the fact that CVSS base scores are already provided in most Common Vulnerabilities and Exposures (CVE) listings by Mitre[17], the National Vulnerability Database[18], and other security advisories. For vulnerabilities that do not have an existing CVSS score, participants then said they prefer a single tool, and that preference would lean towards the CVSS since it is already a globally used industry standard.

[17] https://cve.mitre.org/
[18] https://nvd.nist.gov/

The topic of risk scoring was by far the most prevalent conversation with participants. There is an overwhelming interest across the industry to have a complete risk scoring tool. 88% of the participants said they would use a completely separate alternative vulnerability scoring tool to the CVSS if it provided a more substantial and comprehensive risk-based scoring method.



Several risk management platforms were evaluated during this study (with a focus on identifying ICS/OT applicability). For the purposes of vendor impartiality and scope, the details of that evaluation are not included in this report. However, it was identified that while many current risk management platforms on the market provide CVE data, none of them integrate CVSS scores into their existing risk scoring calculations. Some platforms do not support the use of CVE data or CVSS scores at all. As a result, many end-users rely solely on CVSS scores as their risk priority solution, and other organizations with the resources to do so are working on their own independent ICS/OT risk scoring and prioritization methods and tools.

5 Conclusions

Throughout the entire ICS/OT cybersecurity (cyber risk management) community, risk scoring and risk prioritization is the driving factor behind a significant interest for a more ICS/OT relevant vulnerability scoring solution, and this is supported by the data gathered in this study. The current CVSS calculator provides the ability to adjust local environment variables, making it more risk-based, but the CIA model used by the CVSS does not efficiently satisfy the requirements of most ICS/OT cyber risk management strategies.

While most ICS/OT practitioners would prefer a CVSS calculator that natively provided a more risk-based section better suited for ICS/OT, this most likely won’t be an option for quite some time. As an alternative solution, most participants do support the idea of using of a supplemental tool as long as it focuses on metrics that are relevant to the consequences and impact to ICS/OT.

Ultimately, what participants, and much of the ICS/OT industry as a whole seem to be looking for is a much more comprehensive risk scoring and prioritization solution, rather than just a vulnerability scoring tool. The evolution of the CVSS has gravitated towards this concept with the inclusion and improvement of the adjustable temporal and environmental metrics sections, but consideration for ICS/OT is significantly underrepresented.

Another thing to consider, which was observed throughout many ICS/OT industry forums and conversations, is the subject of "over standardization". Regardless of its ICS/OT deficiencies, the CVSS score is an accepted industry standard, and many industry practitioners have expressed concern about having a separate "industrial" vulnerability score in addition to the CVSS score. As a result, it is important to note that a supplemental ICS/OT vulnerability scoring tool should not produce an alternative score to the CVSS and should not be listed on CVE listings. The CVSS calculator is more than sufficient for providing a base vulnerability score that reflects the characteristics of a vulnerability. An ICS/OT addition to the CVSS, or even a completely separate scoring tool, should be used specifically for adding additional risk-based metrics to enhance the end-users' risk prioritization efforts. The value adjustments required in such a mechanism could only be feasibly done by someone with knowledge of the local environment, and not by the original vulnerability scorer. Therefore, a supplemental ICS/OT addition to the CVSS or a separate tool would not produce a secondary vulnerability score. It would simply improve upon a process, which already part of the current CVSS calculator.

While a more comprehensive ICS/OT risk scoring tool is much larger conversation and endeavor, an ICS/OT addition or supplement to the CVSS should absolutely be risk-focused, rather than just an industrial vulnerability scoring tool. It should incorporate the base CVSS score or provide a mechanism similar to the CVSS calculator to create a base score in the event that a CVE and/or CVSS score does not exist for a vulnerability.

Based on the results of this study, such a mechanism or tool should consider applying the following consequence and impacts for ICS/OT as environmental metrics, which serve as "modifier values" to the base vulnerability score:

- Financial impact
- Health, Safety, and Environment (HSE) impact
- Network segment/zone location
- Access vector
- Patch frequency
- Compensating controls
- Loss of visibility, monitoring, and control of the process
- Impact to production and the reliability of the process

Providing recommendations for the necessary calculations to incorporate these modifier values into a tool is difficult due to the complexities and mathematics involved. It is a process that requires significant adjustment, testing, and fine tuning over time, with the cooperation and feedback from many industry subject matter experts.

The current development progress underway using the IVSS as a conceptual tool can be found in Appendix A of this report.

Finally, the intent of such a tool should ultimately be to enhance ICS/OT end-users' ability to score and prioritize risk using metrics that are specifically relevant to ICS/OT. It should alleviate the burden of trying to solve the complexities of incorporating a generic vulnerability score into a completely separate risk scoring and prioritization strategy.

6 What Next?

The IVSS is an ongoing project to illustrate the potential of a tool created based on industry feedback and the data gathered from this study. Development and support of the IVSS tool will continue and is available to the public to freely use. Whether it inspires ICS/OT integration into the CVSS or exists as a standalone supplement, the goal of the IVSS project is to release version 1 in 2022 (using industry feedback), with the hope that it can provide the ICS/OT community with a viable (free and open source) risk scoring and prioritization tool for industrial environments, as a supplement to the base CVSS score.

To help support ICS/OT integration into CVSS, Clint Bodungen (primary contributor to this study and report, as well as lead contributor to the IVSS project) has been accepted into the CVSS-SIG.

7 Appendix A – IVSS Specifications

The Industrial Vulnerability Scoring System (IVSS) project is in the early stages of development. It is designed to provide supplemental support to the CVSS, to provide a set of adjustable risk-based metrics for ICS/OT. Data resulting from this study, as well as external feedback from ICS/OT subject matter experts, is still being incorporated into IVSS on an on-going basis.

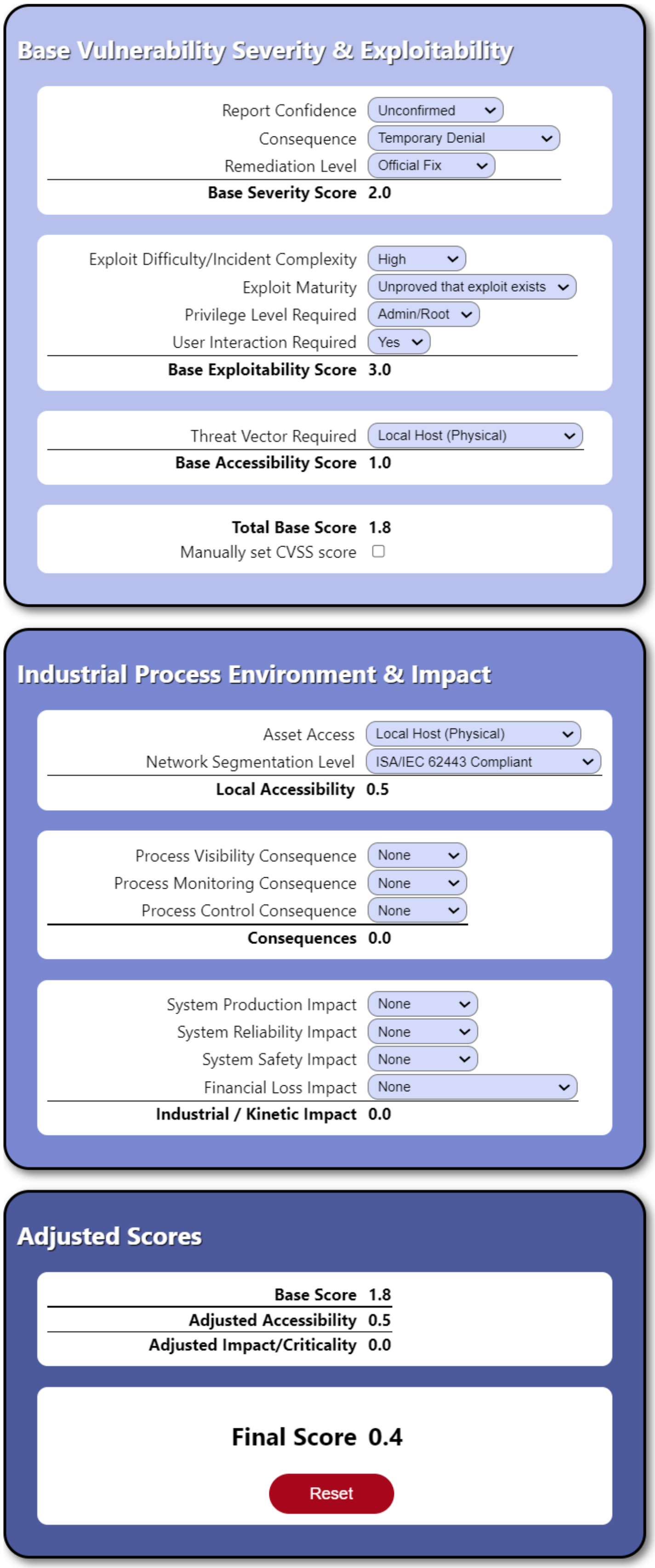
A more comprehensive narrative description of the variables, calculations, and usage will be provided once the most recent feedback and data has been incorporated and as we get closer to a beta release.

An image of the IVSS prototype as well as the current variable and calculation specifications are provided in this appendix. *Note that the sample image and data within the tables are only current as of the time of the release of this report and are still in development*. All features, user interface, data, calculations, and specifications are subject to change on an on-going basis throughout the development process.

The most recent version of the IVSS prototype is free to test and use at:

https://threatgen.com/resources/ivss/

(Example image of the IVSS calculator is on the next page.)



Base Vulnerability Severity & Exploitability

Report Confidence: Unconfirmed
Consequence: Temporary Denial
Remediation Level: Official Fix
Base Severity Score 2.0

Exploit Difficulty/Incident Complexity: High
Exploit Maturity: Unproved that exploit exists
Privilege Level Required: Admin/Root
User Interaction Required: Yes
Base Exploitability Score 3.0

Threat Vector Required: Local Host (Physical)
Base Accessibility Score 1.0

Total Base Score 1.8
Manually set CVSS score ☐

Industrial Process Environment & Impact

Asset Access: Local Host (Physical)
Network Segmentation Level: ISA/IEC 62443 Compliant
Local Accessibility 0.5

Process Visibility Consequence: None
Process Monitoring Consequence: None
Process Control Consequence: None
Consequences 0.0

System Production Impact: None
System Reliability Impact: None
System Safety Impact: None
Financial Loss Impact: None
Industrial / Kinetic Impact 0.0

Adjusted Scores

Base Score 1.8
Adjusted Accessibility 0.5
Adjusted Impact/Criticality 0.0

Final Score 0.4

(NOTE: The parameter definitions and calculations can be found in the tables below and at https://threatgen.com/resources/ivss/)

BASE PARIMETERS

Report Confidence (RC)	
Unconfirmed	0.25
Uncorroborated	0.5
Confirmed	1
Not defined	1

Consequence (BC)	
Temporary Denial	0.25
Data Modification	0.5
Sustained Denial or Loss	0.75
Control	1

Remediation Level (RL)	
Official fix	0
Workaround	0.75
Temporary fix	0.9
Unavailable	1
Not defined	1

Base Severity (BS)

((RC+BC*3+RL)/4)*10

Exploit Difficulty/Incident Complixity (EC)	
High	0.2
Moderate	0.5
Low	1

Exploit Maturity (EX)	
Unproven that exploit exists	0.5
Proof of concept code	0.75
Functional exploit exists	1
Not defined	1

Prvilege Level Required (AU)	
Admin/Root	0.2
User	0.56
None	1
Admin/Root	

User Interaction Required (UI)	
Yes	0.3
No	1

Base Exploitability (BEX)

((EC+EX+AU+UI)/4)*10

Threat Vector Required (AV)	
Local Host (Physical)	0.1
Local Network	0.5
Adjacent or Remote Network	1
Undefined	1

Total Base Score

((BS+BEX+(AV*2))/4)

LOCAL ICS ENVIRONMENT

Asset Access (LA)	
Local Host (Physical)	0.25
Local Network	0.5
Adjacent or Remote Network	1

Network Segmentation Level (CP)	
ISA/IEC 62443 Compliant	0.2
DMZ + Parial ICS Segmentation	0.75
DMZ Only	0.85
None (Flat Network)	1

Local Accessibility (ACC)

(LA*CP)*10

Process Visibility Conseqence (VI)	
None	0
Partial	0.5
Complete	1

Process Monitoring Consequence (MI)	
None	0
Partial	0.5
Complete	1

Process Control Consequences (CI)	
None	0
Partial	0.5
Complete	1

Consequences (CON)

((VI+MI+CI*3)/5)*10

System Production Impact (PI)	

None	0
Low	0.4
Medium	0.7
High	1
Not Defined	1

System Reliability Impact (RI)	
None	0
Low	0.33
Medium	0.66
High	1
Not Defined	1

System Safety Impact (SI)	
None	0
Low	0.5
Medium	0.8
High	1
Not Defined	1

Impact (IMP)

(CD*5*PI*2+RI+SI*6)/14*10

Financial Loss Impact (CD)	
1 - None	0
2 - Low	0.5
3 - Low-medium	0.75
4 - Medium-high	0.9
5 - High	1
Not defined	1

Adjusted Accessibility (ADJACC)

LA

Adjusted Criticality (ADJIMP)

(CON+(IMP*2))/3

Final Score

(BS+ADJIMP*5+ADJACC*10)/16