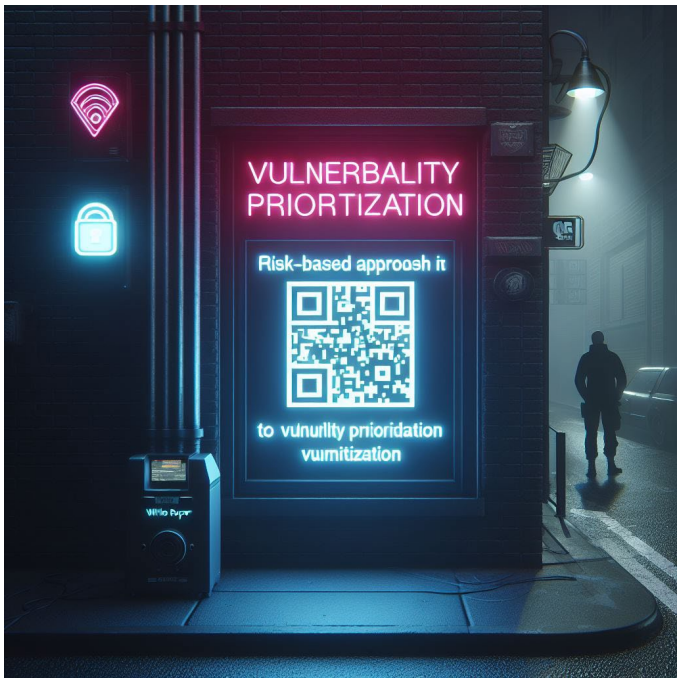

I. Introduction

The document titled "Health-ISAC: Risk-Based Approach to Vulnerability Prioritization" discusses the importance of prioritizing vulnerabilities in cybersecurity management. With over 15,000 vulnerabilities identified in 2023 and 25,227 in 2022, organizations are overwhelmed by the volume of findings and the challenging task of triaging vulnerabilities to determine which to address first.

The paper emphasizes the need for maturing vulnerability management processes and a shift away from traditional severity ratings. It suggests that organizations should implement sustainable frameworks and standards for prioritization in vulnerability management.

This document is set to be meticulously analyzed, with a focus on the multifaceted aspects of vulnerability management within the healthcare sector. The analysis will delve into the strategies and frameworks recommended for effectively prioritizing vulnerabilities.

The document provides a comprehensive and practical guide to vulnerability prioritization. While it has some drawbacks and limitations, it can be a valuable resource for organizations looking to improve their vulnerability management processes.

A. Benefits

- **Risk-Based Approach**: a risk-based approach to vulnerability management can help organizations focus on the most critical vulnerabilities that pose the greatest threat
- **Comprehensive Framework**: a comprehensive framework includes various methods such as Base CVSS Scoring, focusing on known exploited vulnerabilities, considering device context or placement, asset value, compensating controls, and using tools like EPSS (Exploit Prediction Scoring System) and SSVC (Stakeholder-Specific Vulnerability Categorization)
- **Practical Guidance**: The document offers practical guidance on how to implement these methods and tools, making it easier for organizations to adopt these practices

B. Drawbacks

- **Resource Intensive**: Implementing the methods and tools suggested in the document can be resource-intensive, requiring significant time, effort, and expertise
- **Complexity**: The document's approach is complex and may be challenging for smaller organizations or those with less mature security teams to implement

C. Limitations

- **Dependent on Accurate Data**: The effectiveness of the methods and tools suggested in the document is dependent on the availability and accuracy of data. For instance, asset value prioritization requires an accurate and agreed-upon business impact value per company asset
- **Dynamic Threat Landscape**: The document's approach may not account for the dynamic nature of the threat landscape. New vulnerabilities and threats emerge constantly, which may require adjustments to the prioritization framework
- **Human Element**: While the document suggests methods to eliminate the human element from prioritization, human judgment is still crucial in many aspects of vulnerability management. For instance, determining the effectiveness of compensating controls or interpreting the results of tools like EPSS and SSVC requires human expertise
- **Reliance on CVSS Scoring**: The document discusses the use of Common Vulnerability Scoring System (CVSS) as a baseline for vulnerability management. While CVSS is a widely accepted standard, it has been criticized for not accurately reflecting the real-world risk of vulnerabilities. The document acknowledges this and suggests using additional tools like the Exploit Prediction Scoring System (EPSS) and Stakeholder-Specific Vulnerability Categorization (SSVC), but the reliance on CVSS could still be seen as a limitation
- **Lack of Practical Examples**: While the document provides a comprehensive theoretical framework for vulnerability prioritization, it could benefit from more practical examples or case studies to illustrate how these concepts can be applied in real-world scenarios

II. Key Concepts

Risk-based approach covers several key concepts:

- **Using Base CVSS Scoring**: The Common Vulnerability Scoring System (CVSS) is a standard used to rate the severity and exploitability of vulnerabilities. However, only 2-7% of all published vulnerabilities are ever exploited in the wild, often due to a lack of prioritization
- **Focusing on Known Exploited Vulnerabilities**: The paper suggests a more risk-based approach, focusing on known exploited vulnerabilities. The Cybersecurity and Infrastructure Security Agency (CISA) has

released a list of Known Exploit Vulnerabilities (KEV) to help organizations prioritize their remediation efforts

- **Device Context or Placement**: The network location of a device is a critical factor in vulnerability prioritization. Internet-facing vulnerabilities and misconfigurations should always be a priority, while internally-facing assets should fall under an internal service level agreement (SLA) remediation timeline
- **Asset Value**: The value of an asset is another important factor in vulnerability prioritization. Analysts must know the asset's value as they leverage device context and placement
- **Compensating Controls**: Most organizations have layered security controls or defense-in-depth strategies to mitigate attacks. These security controls should make it more difficult to exploit vulnerabilities
- **EPSS – Exploit Prediction Scoring System**: EPSS is a machine-learning model that predicts the likelihood or probability that a vulnerability will be exploited in the wild. It helps defenders prioritize vulnerability remediation efforts more effectively
- **SSVC – Stakeholder-Specific Vulnerability Categorization**: SSVC focuses on values, including the security flaw's exploitation status, its impact on safety, and the prevalence of the affected products. It improves vulnerability management processes and accounts for diverse stakeholders

III. Using Base CVSS Scoring

It discusses the use of the Common Vulnerability Scoring System (CVSS) as a baseline for vulnerability management, particularly for organizations with smaller security teams or those in the early stages of developing a vulnerability management program

- **Base CVSS Scoring as a Starting Point**: For organizations with limited resources or those just starting their vulnerability management program, using the base CVSS scoring to prioritize and remediate all critical and high severity vulnerabilities can be a good starting point. This approach eliminates the need for human judgment in prioritizing vulnerabilities, which can be beneficial for smaller teams or those with multiple responsibilities
- **Limitations of Base CVSS Scoring**: While using base CVSS scoring can be a good starting point, it has its limitations. For instance, remediation teams may be overwhelmed by the sheer number of vulnerabilities they are asked to focus on. Additionally, threat actors may not always exploit the highest severity vulnerabilities and instead chain together multiple exploits of less severe vulnerabilities to gain access to systems
- **Need for a More Risk-Based Approach**: Given the limitations of using base CVSS scoring alone suggests a more risk-based approach that focuses on known exploited vulnerabilities. This approach significantly reduces the number of vulnerabilities that need immediate attention and ensures practitioners focus on vulnerabilities that pose the greatest threat to organizations

The Common Vulnerability Scoring System (CVSS) is a framework used to rate the severity of security vulnerabilities. It uses three groups of metrics to calculate scores: Base, Temporal, and Environmental

- **Base Metrics**: These metrics produce a score ranging from 0 to 10, which reflects the inherent characteristics of a vulnerability that are constant over time and across user environments. They are divided into two groups: Exploitability Metrics (such as Attack Vector, Attack Complexity, Privileges Required, and User Interaction) and Impact Metrics (which measure the impact on Confidentiality, Integrity, and Availability)
- **Temporal Metrics**: These metrics reflect the characteristics of a vulnerability that may change over time but not among user environments. They include Exploit Code Maturity, Remediation Level, and Report Confidence. Temporal metrics are optional and used to produce a temporal score, which is a modification of the Base score
- **Environmental Metrics**: These metrics enable the user to customize the CVSS score depending on the importance of the affected software, hardware, or data in their environment. They include Collateral Damage Potential, Target Distribution, Confidentiality Requirement, Integrity Requirement, and Availability Requirement. Like Temporal metrics, Environmental metrics are optional and used to produce an environmental score, which is a further modification of the Temporal score

The CVSS Base score differs from the Temporal and Environmental scores in that it only considers the inherent, unchanging characteristics of the vulnerability. In contrast, the Temporal score takes into account factors that change over time, such as whether an exploit has been developed or a patch is available. The Environmental score allows for customization based on the importance of the affected assets in a specific user's environment. Therefore, while the Base score is the same for all users, the Temporal and Environmental scores can vary depending on the time and the specific user environment.

The Base, Temporal, and Environmental metrics impact each other in the sense that the Temporal Score is a modification of the Base Score, and the Environmental Score is a modification of the Temporal Score. This means that changes in the Base metrics will affect the Temporal and Environmental scores, and changes in the Temporal metrics will affect the Environmental score. However, changes in the Environmental metrics do not affect the other scores, as it is specific to the user's environment.

The Common Vulnerability Scoring System (CVSS) base score typically does not change over time. It is a static score that represents the severity of a vulnerability based on the characteristics of the vulnerability itself, such as its impact and exploitability. However, the interpretation and application of the CVSS score can change over time based on various factors.

For instance, the CVSS score might be used differently in the context of an organization's vulnerability management process. An organization might prioritize vulnerabilities not just based on their CVSS scores, but also on factors such as whether the vulnerability is being actively exploited, the value of the assets that could be affected, the presence of

compensating controls, and the context of the device where the vulnerability exists.

Moreover, tools like the Exploit Prediction Scoring System (EPSS) and the Stakeholder-Specific Vulnerability Categorization (SSVC) can be used to supplement the CVSS score. EPSS uses a machine-learning model to predict the likelihood that a vulnerability will be exploited in the wild, providing a dynamic perspective on the risk posed by the vulnerability. SSVC, on the other hand, focuses on values including the security flaw's exploitation status, its impact on safety, and the prevalence of the affected products, allowing for a more customized and dynamic approach to vulnerability management.

IV. Focusing on Known Exploited Vulnerabilities

It emphasizes the importance of prioritizing known exploited vulnerabilities in cybersecurity risk management.

- **Known Exploited Vulnerabilities**: The report suggests a risk-based approach that focuses on known exploited vulnerabilities. It cites the Binding Operational Directive 22-01 released by CISA, which aims to reduce the risk of known exploited vulnerabilities. The directive emphasizes that less than 4% of all known vulnerabilities have been used by attackers in the wild, so focusing on these vulnerabilities can significantly reduce the number of vulnerabilities that need immediate attention
- **Prioritization**: The report suggests that known exploited vulnerabilities should be the top priority for remediation. This approach ensures that practitioners focus on vulnerabilities that pose the greatest threat to organizations. A process that keeps an organization safe would likely include focusing on CISA's Known Exploited Vulnerabilities (KEV) list and pivoting to remediate non-exploited vulnerabilities with critical and high severity levels
- **Reduced** Number of Vulnerabilities: This methodology significantly reduces the number of vulnerabilities that need immediate attention. As of July 13, 2023, there were less than 1,000 vulnerabilities on the list. It also ensures practitioners focus on vulnerabilities that pose the greatest threat to organizations
- **Compliance Obligations**: The report also notes that while the directive helps agencies prioritize their remediation work, it does not release them from any compliance obligations, including resolving other vulnerabilities
- **CVSS Scoring**: The report acknowledges that CVSS scoring can still be a part of an organization's vulnerability management efforts, especially with machine-to-machine communication and large-scale automation

Focusing on known exploited vulnerabilities is a critical aspect of vulnerability management. It allows organizations to efficiently allocate resources, reduce risk, develop effective strategies, comply with regulations, prioritize based on threats, and protect valuable assets:

- **Efficient Resource Allocation**: With thousands of vulnerabilities identified each year, organizations often struggle to manage and remediate all of them due to limited resources. Focusing on known exploited vulnerabilities allows organizations to prioritize their efforts and resources on the vulnerabilities that pose the most significant threat
- **Risk Reduction**: Known exploited vulnerabilities are those that have been used by attackers in the wild. By prioritizing these vulnerabilities, organizations can significantly reduce their risk exposure. For instance, a study found that less than 4% of all known vulnerabilities have been used by attackers in the wild
- **Effective Mitigation and Remediation Strategies**: Prioritizing known exploited vulnerabilities supports the development of effective mitigation and remediation strategies. It helps security teams communicate effectively with stakeholders, identify asset value, and develop remediation policies conducive to the continuity of business-critical systems
- **Regulatory Compliance**: Regulatory bodies like the Cybersecurity and Infrastructure Security Agency (CISA) have directives focusing on reducing the risk of known exploited vulnerabilities. Compliance with these directives is another reason to prioritize known exploited vulnerabilities
- **Threat-Based Prioritization**: Focusing on known exploited vulnerabilities allows for a more threat-based approach to vulnerability management. This approach ensures that practitioners focus on vulnerabilities that pose the greatest threat to organizations
- **Asset Protection**: Prioritizing known exploited vulnerabilities helps protect valuable assets. If a device that is of utmost importance to the operation of the business or holds critical information were to be compromised, it could be catastrophic to the organization

V. Device Context or Placement

The network location of devices is significant in the process of vulnerability prioritization.

- **Criticality of Network Location**: This knowledge is crucial for prioritizing vulnerabilities, especially when new CVEs and zero-days are disclosed for internet-facing assets
- **Prioritization of Internet-Facing Vulnerabilities**: Vulnerabilities and misconfigurations on internet-facing devices should be prioritized because they are more accessible to threat actors and can serve as an easy entry point for attacks. These vulnerabilities pose a higher risk of compromise and should be addressed promptly
- **Internal SLA Remediation Timeline**: For systems that are not accessible from the internet, such as internally facing assets, should fall under an internal service level agreement (SLA) remediation timeline. This implies that different SLAs should be established based on the network location of the assets, with internet-facing assets having shorter SLAs than internally-facing ones
- **Lateral Movement Considerations**: When prioritizing internal vulnerabilities, the focus should be on preventing lateral movement within the network. Prioritization should be given to vulnerabilities that could allow an attacker to gain control of a system or move laterally to access sensitive data

- **Use of Vulnerability Priority Ratings**: most vulnerability management tools today incorporate additional scoring features, such as the Exploit Prediction Scoring System (EPSS), to assist analysts in prioritizing vulnerabilities. These tools provide vulnerability priority ratings that help determine which security flaws should be remediated first based on the likelihood of exploitation within the network
- **Risk-Based Approach**: By incorporating the context of device location, organizations can operate in a manner that aligns with a risk-based approach to vulnerability management. This approach ensures that patching teams focus on remediating vulnerabilities based on their attack vector, exploitability, and severity

In the context of vulnerability management, "device context or placement" refers to the network location and role of devices, which is a critical factor in prioritizing vulnerabilities. The placement of a device can significantly affect the risk level of a vulnerability and therefore influence the prioritization for remediation efforts.

A. Examples of Device Context or Placement in Vulnerability Management

- **Emerging Threat Response**: Organizations need to respond quickly to emerging threats or critical vulnerabilities on publicly facing devices. For example, if a new vulnerability is disclosed that affects web servers, those internet-facing servers would be prioritized for patching
- **Internal Web Applications**: While also important, vulnerabilities affecting internal web applications might be addressed after those on internet-facing servers, based on the reduced risk of immediate external exploitation
- **Workstations vs. Servers**: A local privilege escalation vulnerability might be prioritized on workstations over servers if the workstations are more likely to be targeted through phishing emails, considering the context of how the devices are used

VI. ASSET VALUE

It discusses the importance of understanding the value of an asset in the context of vulnerability prioritization

- **Asset Value Importance**: The value of an asset plays a crucial role in vulnerability prioritization. Analysts need to understand the value of an asset in conjunction with its context and placement in the network. This understanding helps in prioritizing vulnerabilities associated with critical assets
- **Ranking System**: Teams can use a ranking system within their application repository to identify critical assets. Vulnerabilities associated with these critical assets should be prioritized for remediation. This approach helps analysts influence decisions to remediate vulnerabilities impacting business-critical assets
- **Business Impact**: If a device that is crucial to the operation of the business or holds critical information were to be compromised, it could be catastrophic for the organization. Therefore, it is recommended to prioritize patching these devices over others. Incorporating business impact into severity weighting provides a more accurate view of risk to the company
- **Configuration Management Database (CMDB)**: To effectively implement this strategy, an accurate and agreed-upon business impact value per company asset is needed. Ideally, this information should be centrally located, such as in a Configuration Management Database (CMDB). Although most industry CMDB products provide an asset discovery solution to help maintain inventory accuracy, it will only be partially absolved of challenges

In vulnerability management, asset value refers to the importance of a particular asset (such as a device, system, or data) to an organization's operations or business continuity. It is a critical factor in vulnerability prioritization, helping security teams decide which vulnerabilities to address first based on the potential impact on the organization's most valuable assets

The calculation of asset value in vulnerability management is not a straightforward process and can vary depending on the organization's specific context and needs. It often involves assessing the asset's role in the organization, the sensitivity of the data it holds, its importance to business operations, and the potential impact on the organization if the asset were to be compromised

Several factors can affect the asset value in vulnerability management:

- **Role of the Asset**: The function of the asset in the organization can greatly influence its value. For example, a server hosting critical applications or sensitive data would typically have a higher asset value than a peripheral device with no access to sensitive information
- **Data Sensitivity**: Assets that store or process sensitive data, such as personally identifiable information (PII), financial data, or proprietary business information, typically have a higher value due to the potential impact of a data breach
- **Business Impact**: The potential impact on business operations if the asset were to be compromised is a significant factor. This could include financial loss, operational disruption, reputational damage, or legal and regulatory consequences
- **Asset Placement or Context**: The location of the asset in the network and its exposure to potential threats can also affect its value. For example, assets that are publicly accessible or located in a demilitarized zone (DMZ) may be considered more valuable due to their increased risk of being targeted by attackers
- **Compensating Controls**: The presence of security controls that could mitigate the impact of a vulnerability can also affect the perceived value of an asset. For example, an asset with robust security controls in place may be considered less valuable from a vulnerability management perspective because the risk of successful exploitation is reduced

In order to effectively prioritize vulnerabilities based on asset value, organizations need to maintain an accurate inventory of their assets and regularly assess their value in the context of the organization's operations and risk tolerance

VII. Compensating Controls

It discusses the role of layered security controls or defense-in-depth strategies in mitigating attacks executed by advanced security threats.

- **Role of Compensating Controls**: Compensating controls are security measures that make it more difficult to exploit vulnerabilities. They are part of an organization's layered security strategy, also known as a defense-in-depth strategy
- **Controversy Over Severity Adjustment**: The practice of adjusting the severity of vulnerabilities based on compensating controls is controversial. Some stakeholders argue for lowering the severity of vulnerabilities under the assumption that the control is effective. However, changing a vulnerability's severity or risk rating without sufficient data can lead to misprioritization and weaken an organization's security posture
- **Testing Compensating Controls**: The report recommends testing the exploitation of vulnerabilities against the company's security stack in a sandboxed environment. This can be done by personnel with red teaming expertise or by using a breach and attack simulation tool to mimic the tactics, techniques, and procedures (TTPs) of the exploitation activities observed in malicious operations. This data can help determine if the severity or risk rating of certain vulnerabilities can be decreased or increased

Compensating controls in vulnerability management are additional security measures put in place to mitigate the risk associated with identified vulnerabilities. They are used when vulnerabilities cannot be immediately remediated due to technical constraints, business requirements, or other factors. Compensating controls can help prioritize vulnerabilities by reducing the risk associated with certain vulnerabilities, allowing organizations to focus on remediating other, higher-risk vulnerabilities first

Compensating controls can take various forms, including:

- **Network Segmentation**: This involves separating a network into multiple segments to limit an attacker's ability to move laterally within the network. If a vulnerability exists in one segment of the network, network segmentation can prevent an attacker from exploiting that vulnerability to access other parts of the network
- **Firewalls and Intrusion Prevention Systems (IPS)**: These tools can detect and block malicious traffic, potentially preventing the exploitation of certain vulnerabilities
- **Multi-factor Authentication (MFA)**: MFA can prevent an attacker from gaining access to a system even if they have obtained valid credentials, thus mitigating the risk associated with vulnerabilities that could lead to credential theft
- **Encryption**: Encrypting data at rest and in transit can reduce the impact of vulnerabilities that could lead to data exposure
- **Regular Patching and Update**s: Regularly updating and patching systems can help to mitigate the risk associated with known vulnerabilities
- **Security Awareness Training**: Training users to recognize and avoid potential security threats can reduce the risk of vulnerabilities being exploited through social engineering attacks

In terms of prioritizing vulnerabilities, compensating controls can be used to lower the risk rating of certain vulnerabilities, allowing organizations to focus on remediating other vulnerabilities first. However, it's important to note that the effectiveness of compensating controls should be regularly tested to ensure they are functioning as expected. This can be done through red teaming exercises or using breach and attack simulation tools.

In addition to compensating controls, other factors that can be used to prioritize vulnerabilities include the severity of the vulnerability, the exploitability of the vulnerability, the value of the asset affected by the vulnerability, and whether the vulnerability is known to be exploited in the wild. Tools like the Exploit Prediction Scoring System (EPSS) and the Stakeholder-Specific Vulnerability Categorization (SSVC) can also be used to help prioritize vulnerabilities

A. Difference between compensating controls and patching in vulnerability management

In the context of vulnerability management, compensating controls and patching are two different strategies used to mitigate the risk associated with identified vulnerabilities.

Patching refers to the process of applying updates to software or systems to fix known vulnerabilities. This is a direct method of addressing vulnerabilities, as it involves modifying the system or software to eliminate the vulnerability. Patching is often the most effective way to prevent exploitation of a vulnerability, but it can also be resource-intensive and disruptive, as it may require systems to be taken offline or restarted. It's also important to note that not all vulnerabilities have available patches, and even when they do, there can be delays in applying them due to testing requirements or operational constraints.

On the other hand, compensating controls are alternative measures implemented to mitigate the risk associated with a vulnerability when it is not feasible or desirable to apply a patch. These controls do not fix the vulnerability itself, but they reduce the risk of exploitation. Examples of compensating controls include network segmentation, firewall rules, intrusion detection systems, and additional monitoring. The use of compensating controls can be controversial, as they do not eliminate the vulnerability and their effectiveness can be difficult to measure. However, they can be a valuable tool in managing risk, particularly in cases where patching is not immediately possible.

While patching directly addresses and eliminates vulnerabilities, compensating controls provide alternative ways to mitigate the risk associated with vulnerabilities when patching is not feasible or desirable. Both strategies are important components of a comprehensive vulnerability management program.

VIII. EPSS – Exploit Prediction Scoring System

The Exploit Prediction Scoring System (EPSS) is a tool that helps prioritize vulnerabilities in cybersecurity. It provides a data-driven, probabilistic assessment of the likelihood of exploitation, which can complement traditional severity ratings and other vulnerability management strategies.

- **Challenges with Traditional Vulnerability Scoring**: Traditional vulnerability scoring systems, such as the Common Vulnerability Scoring System (CVSS), have been criticized for not being sufficient to assess and prioritize risks from vulnerabilities. Only a limited subset of published vulnerabilities is ever observed being exploited in the wild
- **Introduction of EPSS**: The EPSS is an open, data-driven effort that uses a machine-learning model to predict the likelihood or probability that a vulnerability will be exploited in the wild. This assists defenders in prioritizing vulnerability remediation efforts more effectively. EPSS uses data from sources like the MITRE CVE list, data about CVEs such as days since publication, and observations from exploitation-in-the-wild activity from security vendors
- **EPSS Scoring**: The EPSS model produces a probability score between zero and one (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited
- **Comparison with CVSS**: EPSS is not meant to replace CVSS but to complement it. While CVSS provides a severity rating for vulnerabilities, EPSS provides a prediction of the likelihood of exploitation. This additional information can help organizations prioritize their remediation efforts more effectively
- **Use of EPSS in Vulnerability Management**: EPSS can be used in conjunction with other tools and strategies for vulnerability management, such as focusing on known exploited vulnerabilities, considering the context or placement of devices, assessing asset value, and considering compensating controls
- **Stakeholder-Specific Vulnerability Categorization (SSVC)**: SSVC is another tool that can be used in conjunction with EPSS. SSVC focuses on values, including the security flaw's exploitation status, its impact on safety, and the prevalence of the affected products. SSVC improves vulnerability management processes and accounts for diverse stakeholders

A. EPSS Difference

The Exploit Prediction Scoring System (EPSS) is a tool designed to estimate the likelihood that a software vulnerability will be exploited in the wild. Its purpose is to assist network defenders in better prioritizing vulnerability remediation efforts by providing a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

EPSS offers a more nuanced approach to vulnerability management by predicting the likelihood of exploitation, which complements the severity assessment provided by traditional scoring systems like CVSS. This predictive capability can significantly benefit organizations in prioritizing their vulnerability remediation efforts.

EPSS differs from traditional severity ratings, such as the Common Vulnerability Scoring System (CVSS), in several ways:

- **Predictive Nature**: EPSS is predictive, providing a probability score based on the likelihood of exploitation, whereas CVSS provides a severity score based on the intrinsic characteristics of a vulnerability
- **Data-Driven Approach**: EPSS uses a data-driven effort that incorporates current threat information from CVE and real-world exploit data, which is not the case with CVSS severity ratings
- **Machine Learning Model**: EPSS employs a machine-learning model to predict exploit likelihood, using data from sources like the MITRE CVE list and observations from exploitation-in-the-wild activity from security vendors

B. Benefits

Benefits of using EPSS in vulnerability management include:

- **Efficient Prioritization**: EPSS helps organizations prioritize vulnerabilities that pose the most risk and are most likely to be exploited, enabling them to allocate resources more effectively
- **Complement to CVSS**: EPSS can be used alongside CVSS to provide a more comprehensive view of vulnerabilities, considering both the severity and the likelihood of exploitation
- **Reduction in Remediation Effort**: By focusing on vulnerabilities with a higher probability of being exploited, organizations can reduce the number of vulnerabilities they need to address, saving time and effort.

IX. SSVC – Stakeholder-Specific Vulnerability Categorization

It discusses a methodology for prioritizing vulnerabilities based on various factors beyond just severity scores. SSVC is a flexible, customizable, and evidence-based approach to vulnerability prioritization that takes into account a variety of factors beyond just severity scores. It helps organizations make informed decisions about which vulnerabilities to address first, based on their specific context and risk tolerance.

- **SSVC Overview**: SSVC is a vulnerability analysis methodology developed by Carnegie Mellon University's Software Engineering Institute in coordination with the US Cybersecurity and Infrastructure Security Agency (CISA). It operates as a decision tree that allows for flexibility in its application, and it accounts for diverse stakeholders.
- **SSVC Decision Points**: SSVC uses a decision tree to determine the response to a vulnerability. The possible outcomes are "Track", "Track*", "Attend", and "Act". Each outcome has a recommended remediation timeline, ranging from standard update timelines ("Track" and "Track*") to immediate action ("Act").
- **Customizability**: SSVC is customizable, helping analysts decide on vulnerability response actions consistent with maintaining the confidentiality, integrity, and availability of enterprise systems as agreed upon with leadership. It is a dynamically applied

concept, with new versions released to recognize improvements and integrate feedback.

- **Focus on Values**: SSVC focuses on values, including the security flaw's exploitation status, its impact on safety, and the prevalence of the affected products. It improves vulnerability management processes by considering these factors.
- **Evidence-Based Decisions**: SSVC decisions are based on a logical combination of triggers set by leadership in response to factors such as the vulnerability's state of exploitation, the level of difficulty for an adversary to exploit it, and its impact on public safety. Analysts collect evidence of the relevant triggers and use the decision tree's logic to establish triage priority decisions.
- **Beyond Base Scores**: SSVC goes beyond just base scores as a stand-alone prioritization method. It helps organizations efficiently prioritize and triage vulnerabilities while navigating the uncertainties of what issues to address first.

A. Key Components of the SSVC Methodology

The Stakeholder-Specific Vulnerability Categorization (SSVC) methodology is a decision-tree-based approach developed by Carnegie Mellon University's Software Engineering Institute in coordination with the US Cybersecurity and Infrastructure Security Agency (CISA). The key components of the SSVC methodology include:

- **Decision Points**: SSVC uses a decision tree with decision points that lead to different outcomes based on the analysis of the vulnerability. These decision points include the state of exploitation, technical impact, automatability, mission prevalence, and public well-being impact.
- **Possible Outcomes**: The decision tree leads to one of four possible outcomes: Track, Track*, Attend, and Act. Each outcome has a recommended remediation timeline, with "Act" requiring immediate action.
- **Customizability**: SSVC is designed to be customizable, allowing organizations to tailor the decision-making process to their specific needs and concerns.
- **Evidence-Based Decisions**: Decisions within SSVC are made based on evidence regarding the vulnerability's exploitation status, difficulty of exploitation, and impact on public safety.
- **Dynamic Application**: SSVC is intended to be a dynamically applied concept, with new versions released to incorporate improvements and feedback.

B. Using SSVC to Prioritize Vulnerabilities

SSVC can be used to prioritize vulnerabilities in an effective and efficient way by

- **Assessing Impact**: Analyzing the impact of a vulnerability on the organization's operations and the public well-being to determine the urgency of remediation.
- **Evaluating Exploitation Status**: Considering whether there is active exploitation or proof of concept available for the vulnerability.
- **Determining Automatability**: Assessing if the vulnerability is self-propagating or requires additional steps for an attacker to exploit.
- **Considering Mission Prevalence**: Evaluating how prevalent the affected product is within the organization and its importance to business continuity.
- **Making Informed Decisions**: Using the decision tree to make informed decisions about which vulnerabilities to address first, based on the organization's specific exposure level and recommended actions.

C. Difference between SSVC and traditional severity ratings in vulnerability management

Traditional severity ratings in vulnerability management, such as the Common Vulnerability Scoring System (CVSS), provide a numerical score to indicate the severity of a vulnerability. These scores are based on a set of metrics that include the attack vector, attack complexity, privileges required, and user interaction, among others. However, these traditional ratings have been criticized for not being sufficient to assess and prioritize risks from vulnerabilities, as they do not consider whether a vulnerability has been exploited in the wild.

On the other hand, the Stakeholder-Specific Vulnerability Categorization (SSVC) is a more dynamic and flexible approach to vulnerability management. SSVC focuses on values, including the security flaw's exploitation status, its impact on safety, and the prevalence of the affected products. It operates as a decision tree that allows for flexibility in its application, enabling organizations to customize it to their specific needs. SSVC provides a more comprehensive view of the risk associated with a vulnerability by considering factors such as the state of exploitation, technical impact, mission prevalence, and public well-being.

While traditional severity ratings provide a standardized measure of the severity of a vulnerability, they do not take into account whether the vulnerability is being exploited or its impact on the organization. SSVC, on the other hand, provides a more comprehensive and customizable approach to vulnerability management by considering a wider range of factors.

D. Scoring decisions in the SSVC methodology

The Stakeholder-Specific Vulnerability Categorization (SSVC) methodology is a decision-making process for vulnerability response actions. It was developed by Carnegie Mellon University's Software Engineering Institute in coordination with the US Cybersecurity and Infrastructure Security Agency (CISA). The SSVC methodology provides four scoring decisions, which are:

- **Track**: The vulnerability does not currently require action, but the organization should continue to monitor it and reassess if new information becomes available. CISA recommends remediating Track vulnerabilities within standard update timelines.
- **Track***: The vulnerability has specific characteristics that may require closer monitoring for changes. CISA recommends remediating Track* vulnerabilities within standard update timelines.
- **Attend**: The vulnerability requires attention from the organization's internal, supervisory-level individuals.

Necessary actions include requesting assistance or information about the vulnerability and may involve publishing a notification either internally and/or externally. CISA recommends remediating Attend vulnerabilities sooner than standard update timelines.

- **Act**: The vulnerability requires attention from the organization's internal, supervisory-level, and leadership-level individuals. Necessary actions include requesting assistance or information about the vulnerability, as well as publishing a notification either internally and/or externally. Typically, internal groups would meet to determine the overall response and then execute agreed upon actions. CISA recommends remediating Act vulnerabilities as soon as possible.

E. Examples of SSVC

Here are examples of how SSVC can be applied in vulnerability management:

- **Customized Decision Tree**: SSVC uses a decision tree that is tailored to the organization's needs. For example, an organization can customize the decision tree to focus on factors such as the vulnerability's exploitation status, its impact on safety, and the prevalence of the affected products
- **Possible Outcomes**: The SSVC decision tree leads to one of four possible outcomes: Track, Track*, Attend, and Act. Each outcome has a recommended remediation timeline, with "Act" requiring immediate action. This helps organizations to prioritize vulnerabilities based on the level of attention they require
- **Evidence-Based Decisions**: Decisions within SSVC are made based on evidence regarding the vulnerability's exploitation status, difficulty of exploitation, and impact on public safety. For instance, if a vulnerability is being actively exploited with a high technical impact, the decision might be to "Act" immediately
- **Practical Use Case**: A practical example provided in the document is the prioritization response to the Citrix ShareFile vulnerability, identified as CVE-2023-24489. Using SSVC, an organization would likely choose the "Act" value after running information collected by analysts against the decision points and associated values. This decision is influenced by the existence of proof-of-concept code, evidence of targeted attacks, and in-the-wild exploitation
- **Public Well-Being**: SSVC also considers the potential impact on public well-being. For example, if a vulnerability could lead to physical harm or expose sensitive payment information, it would likely be prioritized for immediate action
- **Mission Prevalence**: The decision tree includes an assessment of how prevalent the affected product is within the organization and its importance to business continuity. This helps to prioritize vulnerabilities that could have an impact on the organization's operations

X. METRICS

It discusses the role of metrics in evaluating and improving a vulnerability management program. It emphasizes the importance of using detailed and informative metrics to assess the effectiveness of a vulnerability management program. By focusing on key risk indicators and compartmentalizing metrics, organizations can gain actionable insights and prioritize remediation efforts more effectively.

- **Metrics as Indicators**: Metrics are essential for highlighting the effectiveness of a vulnerability management program and identifying areas that need improvement. They provide a way to measure the program's performance and guide strategic decisions
- **Beyond Severity Counts**: Simply counting the number of critical, high, medium, and low severity vulnerabilities is not enough to determine if remediation efforts are meeting goals. Metrics should be more nuanced and informative
- **Compartmentalization of Metrics**: Metrics should be compartmentalized by technology, placement on the network, and the Service Level Agreement (SLA) outlined in the company policy. This helps to identify specific areas that require improvement
- **Focus on Known Exploited Vulnerabilities**: Distinguishing between known exploited vulnerabilities and those not currently exploited can reduce noise and direct teams to remediation efforts that need more visibility
- **Key Risk Indicators vs. Key Performance Indicators**: Organizations should focus on key risk indicators rather than just key performance indicators. This approach highlights specific insights obtained from vulnerability data, which can be more actionable
- **Example of Risk-Based Metrics**: An example provided in the document is the comparison of remediation times for vulnerabilities on different platforms, such as Chrome and Edge. This comparison can reveal which platform poses a higher level of risk based on the time it takes to remediate vulnerabilities
- **Actionable Insights**: Performance metrics should be used to show areas of risk, allowing organizations to take actionable steps rather than just tracking individual vulnerabilities