Vulnerability Risk Assessment With Saner

Security investments are hard to justify. The right amount of security at the right cost is possible only if information needed to make those decisions are available. Software vulnerabilities are ubiquitous and most cyber-attacks use these vulnerabilities. SecPod Saner uses Common Vulnerability Scoring System to provide this crucial information on vulnerabilities enabling intelligent security decisions in the enterprise.

Introduction

Risk is an inalienable fact of life. It is so in the Cyber world as well. Understanding sources of risk and taking meaningful steps to mitigate them is essential for business continuity. Good mitigation strategy reduces available opportunity to the attacker thereby making the organisation safer.

Perpetrating cyber security breaches has become very easy. In fact, hacker tools are available for purchase and requires little sophistication to use. Most of these tools use vulnerabilities that are invariably present in commercial software. These attacks can potentially compromise the entire organisation.

Vulnerabilities are software defects that lend themselves to exploits by attackers. We will not dwell much on why these defects remain in released software, suffice it to say that they are difficult to detect and fix during the usual software release cycle. With the constant effort of dedicated security researchers and vigilant users, these defects get detected and reported to the vendors. Vendors release a corrected version of the software in the form of a patch. Once the patch is applied for a particular vulnerability, it cannot be exploited further.

Let us look at some numbers in order to get an idea of the extent of the problem. NIST (National Institute of Standards and Technology) maintains a database of all vulnerabilities detected in most popular software applications and Operating Systems. This number today stands over 65,000! Every day about 22 vulnerabilities were reported in 2014. Usually, soon after the vulnerabilities are made public, patches are available.

It is entirely possible that these vulnerabilities are known to criminals before they become either known to the vendors or the public. In such a case there is a time frame when vulnerabilities can be exploited by criminals before a remedy is available. This presents a great risk to all organisations.

Publicly disclosed vulnerabilities that remain unpatched present a greater risk to the system and thereby to the organisation. However, organisations often tend to postpone applying a patch, even when one is available. Such decisions are made based on a risk analysis, weighing the increased risk due to the presence of vulnerabilities and the impact of applying the patch on the organisation. For example, if the exploitability of a vulnerability is very low and the estimated impact of a compromise is minimal, patching to remove such a vulnerability might be an overhead at best, and may result in some broken functionality at its worst. Such an analysis requires detailed information on all vulnerabilities present and the risk they pose to the organisation.

SecPod Saner uses Common Vulnerability Scoring System (CVSS) to provide comprehensive information on the nature of vulnerabilities present in an organisation. This information is crucial in security decision making.

In principle, applying patches, as soon as they are available, protects systems from attacks based on those specific vulnerabilities. This reduces the risk of cyber-attacks on those systems. Risk is effectively the product of the probability of an adverse event occurring and the likely impact of the event when it occurs.

Risk = Probability of an adverse event materialising * estimated impact of the event

Determination of probability of occurrence is largely heuristic. A common route used by attackers is the exploitation of vulnerabilities in applications present in the organisation. Common Vulnerability Scoring System (CVSS) provides a framework to characterise vulnerabilities that helps in determining the threat they pose. While no scheme can take into account circumstances such as the motivation of the attacker, CVSS provides a set of metrics that help determine the exploitability of the vulnerability. This helps in estimating the probability of an adverse incident involving that particular vulnerability. Such information is valuable in determining the potential damage and making decisions on if applying a patch can be postponed.

CVSS metrics

Although occurrence of an incident depends not only on the vulnerability but also on circumstances outside of it, there are certain properties inherent to the vulnerabilities. CVSS scores provide a way of characterising vulnerabilities that helps in estimating threat posed by vulnerabilities. Under the custodial care of Forum for Incident Response and Security Team is an open standard for characterising vulnerabilities.

CVSS scores are based on three groups of properties – Base, Temporal and Environmental. Base properties are independent of user environments and does not change with time. Temporal characteristics are those that tend to change with time and environmental characteristics depend on the circumstances of the user.

While Base metrics are sufficient for most purposes, further refinement of the base score is possible in some cases by adding temporal metrics. Temporal metrics are optional. Both Base metrics and Temporal metrics are assigned by security analysts, product vendors or application vendors.

Further refinement, if necessary, is achieved by adding environmental information to Base and Temporal metrics. This refinement is done by the user as only the user can know the environment in which the vulnerable application runs.

CVSS Base Metrics

CVSS base group of metrics encapsulates fundamental properties of a vulnerability that are independent of user environments and time. It captures two major categories of properties – the access method to launch an attack and the potential impact of a successful attack. The base metric is a score between 0 and 10 and a "vector" that describes how the score was arrived at.

Measuring the Ease of Attack

Base metric captures values for method of access, the ease of access once the attacker has gained access to the system and if any authentication is required to launch an attack.

Access Vector captures whether physical access to the system is required or it can be exploited over the network. Its values can be Local, Adjacent Network and Network. Network access provides the easiest means of exploitation (hence a high score) and Local access implies the hardest (and hence a low score).

Access Complexity captures the level of difficulty in launching an attack using the vulnerability, after the attacker has gained access to the system. If specialised access conditions are required complexity is High (and a low score) and if the configuration allows the attacker to access a wide range of resources easily with no special extenuating circumstances the complexity is Low (and the score high).

Authentication is an extra hurdle to the attacker. If the vulnerability allows access without any further authentication that would pose no barrier to the attacker resulting in a High CVSS score. If multiple authentications are required the CVSS score would be Low.

Measuring the Potential Impact of an Attack

The second set of metrics that determine the CVSS Score measure the potential impact of an attack. It is measured in terms of its impact of Confidentiality, Availability and Integrity.

Confidentiality impact ranges from None to Partial to Complete with an increasing score form Low to High. Similarly, if likely impact of an attack using a vulnerability on Availability is None, it attracts a Low score and Complete attracts a High score. As with Confidentiality and Availability, impact on Integrity is measured similarly with None resulting in a Low score and Complete resulting in a High Score.

CVSS Temporal Metrics

Temporal Metrics capture characteristics of vulnerabilities that change over time. They are not strictly necessary, but when present provides additional insights on the nature of vulnerabilities. These metrics capture details such as the exploitability of the vulnerability, availability of remediation and the confidence level associated with the reported vulnerability.

The values of Exploitability ranges through Unproven, PoC, Functional, High and Not Defined. Not defined is an indication to ignore the metric and from Unproven to High the score gets progressively higher.

Remediation Level ranges through Official Fix, Temporary Fix, Work Around, Unavailable to Not Defined. Like before Not Defined is an indication to ignore the metric the score gets progressively higher from Official Fix to Unavailable.

Report Confidence measures the level of trustworthiness of the sources of reported vulnerabilities. Its value ranges through Unconfirmed, Uncorroborated, Confirmed and Not Defined. The scores increase from Unconfirmed to Confirmed and as above, Not Defined is an indication to skip this metric.

Environmental Metrics

This set of metrics captures the specific details of the environment in which the attack is likely to occur. Since the information required to arrive at this metric is user specific, users are expected to provide the values in determining this category of properties of vulnerabilities. These metrics allow the users to modify the score depending on their specific environment. These metrics include Collateral Damage Potential, Security Requirements (confidentiality, Availability and Integrity) and Target Distribution.

Collatera Damage potential, measures the possibility of loss of life, physical assets, financial loss, productivity loss etc. Its values run through None, Low, Low-Medium, Medium-High, High and Not Defined. Not Defined implies that the value has no effect on the score.

Security Requirements is a metric that allows the user to customise the impact of an attack on Confidentiality, Availability and Integrity. It can take Low, Medium, High and Not Defined as values.

Target Distribution is a measure of the percentage of the systems impacted by an attack. Its values run through Low (1-25% of the systems in the environment are potentially impacted), Medium (25-75% of the systems are potentially impacted), High (75 -100% of the systems are potentially impacted) and Not Defined (indicating that the metric should be ignored).

SecPod Saner and Security Intelligence

Saner scans all endpoint systems in the organisation and provides the capability to remediate systems without manual intervention. Given that every day more than 22 vulnerabilities are reported, it is imperative that such scans be run daily. Conventional scanners that look for vulnerabilities choke the bandwidth in the organisation while running a scan. With agent based scanning, Saner scans all systems under 5 minutes. This makes it possible to run Saner every day and ensure enterprise is safe from exploits and consequent losses.

At the beginning of this article we talked about the importance of reliable information for informed decision making in security investments. In order to make such decisions, it is important to understand risk exposure as best as possible. With its CVSS based scores for each vulnerability detected and comprehensive reporting, Saner provides this crucial information to CISOs and IT managers.

While complete automation of remediation is entirely possible using Saner, it may not be desirable under all circumstances. Saner provides the right information to enable managers to make informed decisions on security. Allocating right resources requires quality information and efficiency of operations demands automation. Reliability at the right cost is of utmost importance.

In summary, it is critical for CISOs and IT managers to have the right kind of information to make intelligent decisions on security investments. Such decisions depend critically on the quality, reliability and the relevance of the information available. SecPod Saner, with its CVSS based scores for vulnerability provides comprehensive information about all vulnerabilities in an enterprise. Using the reports generated by Saner, making decisions become a routine matter.

About Us

Founded in 2008 and headquartered in Bangalore with operations in USA, SecPod Technologies creates cutting edge products to ensure endpoint security. We strongly believe in the principle 'Strong Defense, Not a Weak Cure' and our product Saner Business reflects this ideology by proactively detecting and eliminating vulnerabilities before they can be exploited. We have been entrusted by Enterprise and mid level organizations in various verticals including Government, Healthcare and IT/ITES .

Contact Us

Web: www.secpod.com   Tel: +91-80-4121 4020

Email: info@secpod.com   +1-918-625-3023