2020 STATE OF VULNERABILITY MANAGEMENT REPORT

TABLE OF CONTENTS

INTRODUCTION

The State and Maturity of Vulnerability Risk Management has indeed evolved over the past few years.

From simple routine vulnerability scanning with the sole objective of gathering as much vulnerability information as possible to a highly structured and independent field of cyber security, the vulnerability risk management field has expanded its reach to the threat management and modeling fields, with the purpose of predicting which vulnerability conditions could facilitate a successful security breach into the organization.

For the purpose of documenting the vulnerability management field growth, NopSec periodically issues a State of Vulnerability Management Report – the last report was published in August 2018 - often inspired by security technology innovations, new offensive security techniques and news-worthy security breaches.

In building this year's report, NopSec examined anonymized data collected from clients using NopSec Unified VRM® (Vulnerability Risk Management) platform, the company's flagship risk-based vulnerability management platform. The intention of this year's report is to go through the main areas of the vulnerability risk management process using Unified VRM metrics dashboards as a blueprint to explore the population of vulnerabilities gathered from our client base. The data was aggregated anonymously and sheds light on the typical vulnerabilities management practices and key performance indicators of a well-formed vulnerability risk management program.

This year's report is going through the main areas of a well-structured vulnerability risk management program, including:

- Asset management and inventory
- Vulnerability assessment
- Threat-based prioritization
- Remediation and patch management
- The vulnerability landscape based on NopSec client data
- Lesson learned for program improvement and conclusions

The objective of this report is to reflect on the different vulnerability management phases and their current maturity and trends through a cumulative dashboard view of the Unified VRM SaaS solution, anonymously accumulating vulnerability and asset data from January 2019 to the present date. These cumulative views will reveal trends and considerations about vulnerability management practices and overall program maturity.

At the end of the analysis, we will draw conclusions on the maturity of current vulnerability management practices as found in the sample of client organizations analyzed.

It is important to note that our analysis comes from a non-random sample set from our clients' data - as such, we do not claim that this is a definitive analysis of all possible vulnerabilities and threats that an average organization could face. The possibility of sample bias exists, and this should be kept in mind throughout the report. However, we believe that our research offers important insight into how companies in various industries prioritize vulnerabilities, the universal weaknesses that companies across different industries share, and factors that should be incorporated into a comprehensive threat detection and remediation program.

CROWDSTRIKE

OVERVIEW

With so many organizations forced to rapidly move employees en masse to remote working environments, security teams face a critical challenge – protecting their work-from-anywhere employees from unknown weaknesses and vulnerability in their systems. The loss of visibility and control of these systems and data could result in weakened defenses, which could lead to an opportunity for an attacker. In addition to incomplete and outdated data, cyber criminals are capitalizing on human error and misconfigurations, coupled with out-dated, non-compliant and exposed systems.

IMPORTANCE OF WORKLOADS HYGIENE

The basics of user awareness, asset and vulnerability management, and secure configurations continue to serve as the foundation for a strong cybersecurity program. CrowdStrike Global Threat Report recommends that organizations regularly review and improve their standard security controls, including the following:

- **Asset management** and software inventory are crucial to ensuring that organizations understand their own footprint and exposure.
- **Vulnerability and patch management** can verify that known vulnerabilities and insecure configurations are identified, prioritized and remediated.
- **Threat-based prioritization** for analysts fatigued by alerts to help them identify the vulnerabilities that correlate to real and urgent threats and separate them from the non-critical vulnerabilities
- **User awareness programs** should be initiated to combat the continued threat of phishing and related social engineering techniques
- **Strong Multifactor Authentication (MFA), robust privilege access management, password protection** are key cybersecurity measures required to stop today's attackers from hiding their malicious activities and deepening their foothold.

CROWDSTRIKE

About CrowdStrike Falcon Platform

The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates trillions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security. With CrowdStrike, you can be confident that your organization is finally protected from cyberattacks — known or unknown, with or without malware.

ASSET MANAGEMENT & INVENTORY

Asset inventory management means managing the complete life-cycle of all IT assets. Effective asset inventory management ensures that every server, workstation, mobile device, IoT device, router, switch, application, and more, are accounted for and correctly evaluated in terms of value and impact if the asset were ever lost or stolen. It also involves searching and finding assets present in the “Shadow IT” areas - assets that are not accounted for and never discovered in the current asset inventory management.

WHY ASSET MANAGEMENT IN VULNERABILITY MANAGEMENT IS CRITICAL

DATA ANALYSIS

Starting with asset inventory management and asset risk, the cumulative asset population data suggests that most of the asset risk (vulnerability risk + asset value) lies in the Low category (Risk Grade “A”), with about 20,000 assets (about 10%) in the High and Critical categories (Risk Grades “C” and D”). As you can see, the vulnerability prioritization works for those most critical assets and risky vulnerabilities, thus reducing the number of total assets in these critical risk categories. For these assets, the underlying message could be: focus your remedial actions on assets that matter the most to your business.

Asset Risk

A	129,188
B	62,337
C	20,142
D	96
Grand Total	211,763

As for the criticality of the asset, the Unified VRM system is capable of programmatically assigning an asset value based on the asset’s characteristics, the base OS, the open ports and the asset’s exposure to public or private networks. Most of the assets are assigned a Medium value with few exceptions including domain controllers, LDAP servers, DNS and Web servers, database and file servers, etc. which are assigned higher values.

Assets by Criticality

Critical	8,793
High	3,182
Medium	198,992
Low	272
None	524
Grand Total	211,763

As you can see, most of the assets in networks are in the Medium value category with Critical and High values categories in second and third position respectively.

ASSET MANAGEMENT & INVENTORY

LESSONS LEARNED

Customers are largely aware of the importance of considering asset management in Vulnerability Management. This is evidenced through NopSec's surveying and Technical Account Management program which provides training and education in these areas. In spite of this, most customers still do not change the default asset values. From interviewing a sample of NopSec customers, we were able to ascertain a trend as to why this is. These reasons are outlined below:

1. Information Security teams lack business context to assign application criticality.
    a. Whilst infosec teams are made aware of the most critical business applications, further granularity of less critical applications is not provided to them. Infosec teams are unable to decipher if a non-critical business application should be labeled as "High", "Medium", or "Low". This can be remediated through increased transparency.
1. IT assets are living shorter life cycles.
    a. Organizations have shifted from testing the infrastructure as code (IaC) to IaC first. IT assets built from code are faster to deploy and as a result are being used as ephemeral assets.
    b. Cloud native infrastructure is built to be on-demand to allow for vertical scaling based on a master image.
    c. Ephemeral assets create a continual asynchronous "race" to assigning asset values which is very challenging for IT teams.

Customers that use NopSec's automatic asset value algorithm have reduced business critical risk four times greater than customers relying on manual processes. NopSec's automatic asset value system enables organzation's IT teams to focus on remediation for the business or mission critical assets, delivering direct security value.

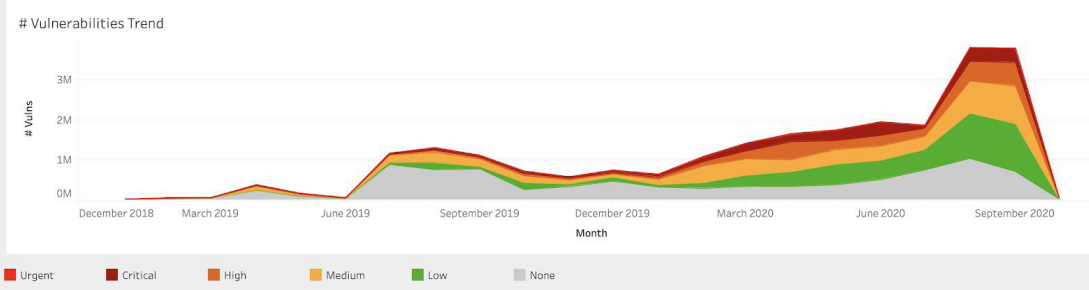
VULNERABILITY DETECTION

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if a system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if needed.

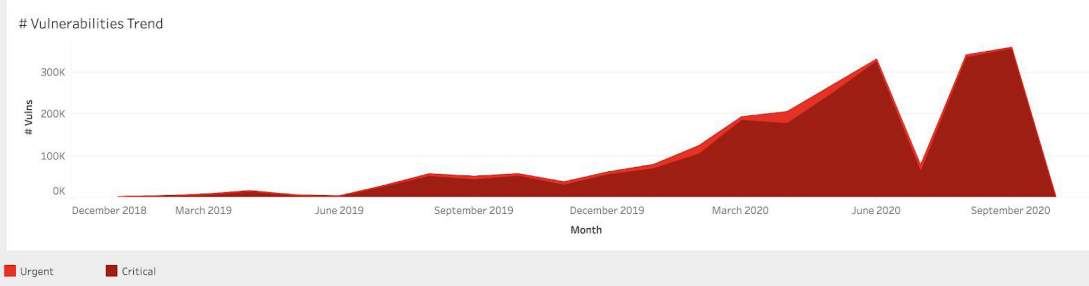
According to the National Institute of Standards and Technology (NIST), “in computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can give access to a system weakness (public or private exploit tool). In this frame, vulnerabilities are also known as the organization’s attack surface”.

First, let’s start with an analysis of vulnerability detection trends by risk.

Below is a chart depicting trends of vulnerability totals by risk level. General increases of vulnerabilities over time are typical for organizations maturing their vulnerability management program. Additional scanners or agents get deployed and more vulnerabilities get discovered, with an overall trend toward the net increase of vulnerabilities, with total vulnerabilities opened exceeding the total vulnerabilities remediated.



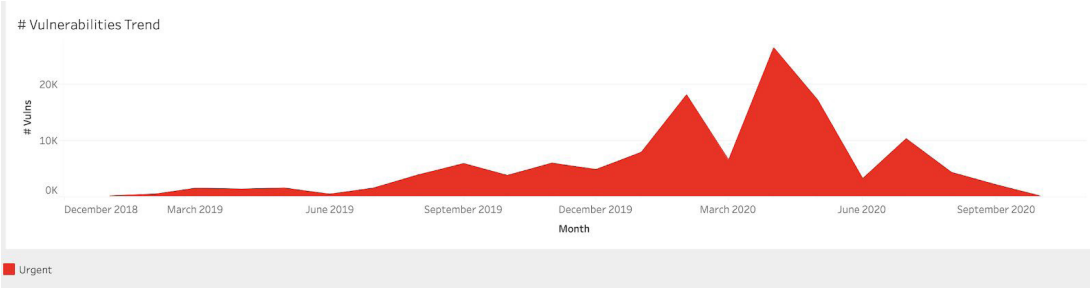
Interesting trends emerge when exclusively reviewing Critical and Urgent vulnerabilities.



Urgent and Critical vulnerabilities account for far fewer vulnerabilities (hundreds of thousands) when compared to the vulnerabilities of lesser severity levels (in the millions). NopSec risk prioritization, especially in the Urgent, high-threat category works at reducing the total number of vulnerabilities to be remediated with urgency. And that always brings back “sanity” in an organization’s vulnerability management “minds”, knowing that they can focus on the vulnerabilities representing the most risk on their assets that matter the most.

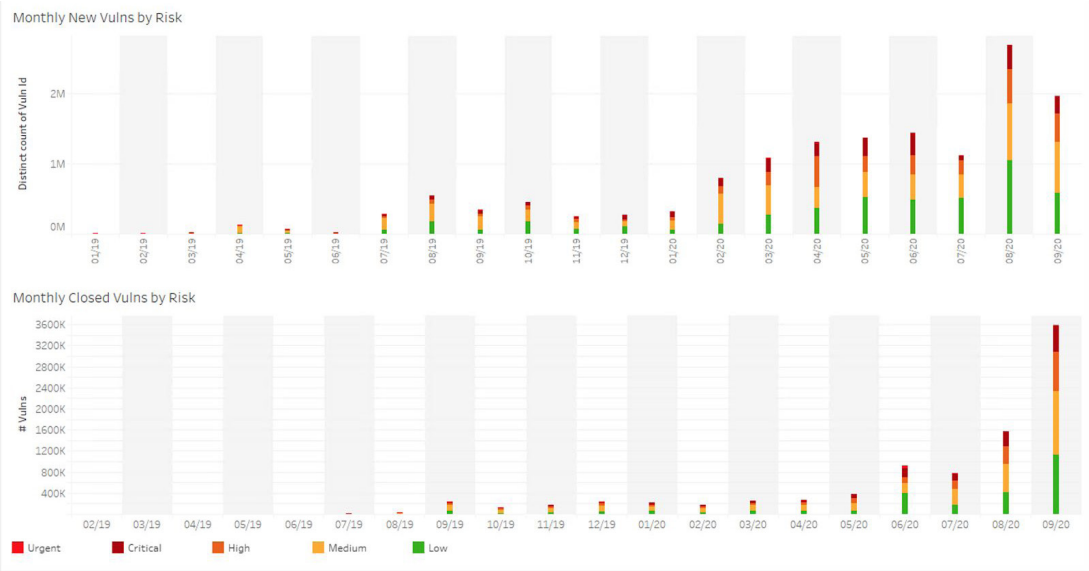
VULNERABILITY DETECTION

The Urgent category includes the vulnerabilities directly correlated with Malware and targeted attacks as suggested by threat intelligence feeds. If we look at the Urgent category only, the number drops even further to a manageable number of patchable vulnerabilities, in the tens of thousands.



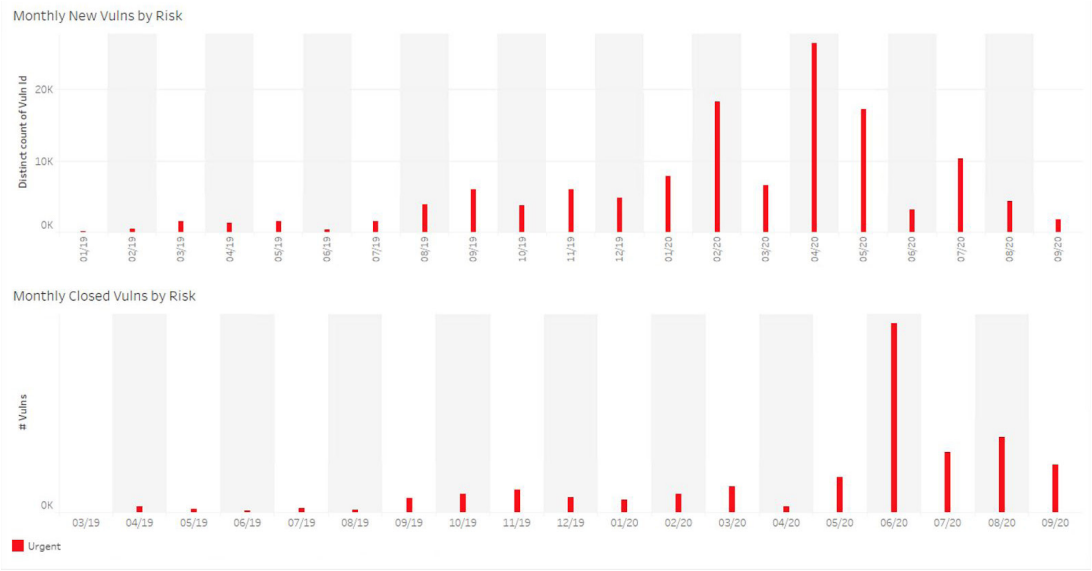
In total, the highest number of prioritized vulnerabilities that are correlated to malware and targeted attacks are around 26,000, instead of several hundreds of thousands of critical vulnerabilities and about a million of high risk vulnerabilities. Again, this shows that overall, NopSec's prioritization machine learning algorithm does its job in reducing workload and optimally narrowing the scope for remediation.

In terms of monthly trends of open and closed vulnerabilities by risk score, the vulnerability trends are recurring, with the spring and summer months being more active in terms of open and closed vulnerabilities.



VULNERABILITY DETECTION

These trends are confirmed when we consider only the Urgent vulnerabilities category, as depicted in the chart below.



Moreover, the same trend has also been confirmed empirically with a flurry of vulnerability disclosures from June through September in the year 2020.

TAKEAWAY

Urgent and Critical vulnerabilities are not predictable. This requires a VRM program to be able to stop and reprioritize what's new and important immediately through an emergency patch management and remediation program. This is generally an anti-pattern when it comes to VRM programs. VRM programs are typically built to be sustainable processes. Unified VRM enables customers to be prepared for these critical surprise vulnerabilities through proactive prioritization and automated remediation. The recommendation is to tightly coupled Security Operations Center (SOC) processes with Urgent vulnerability management discoveries.

THREAT-BASED PRIORITIZATION

Vuln Risk

Urgent	●	19,563
Critical	●	666,239
High	●	964,838
Medium	●	1,782,628
Low	●	2,360,122
None	●	4,394,816
Grand Total	●	10,188,206

Threat-based prioritization represents NopSec Unified VRM differentiator compared to other “brick-and-mortar” vulnerability management solutions. If you compare the total number of vulnerabilities with the number of vulnerabilities factually correlated with threats and potential threats, you can see clearly your attack surface and the remediation efforts that you should focus on.

The total number of prioritized vulnerabilities correlated to real threats and targeted attacks drops from millions to only about nineteen thousand real Urgent vulnerabilities in aggregate. Active threat and potential threat vulnerabilities are about a million in total compared to a little more than nine million for non-threat vulnerabilities.

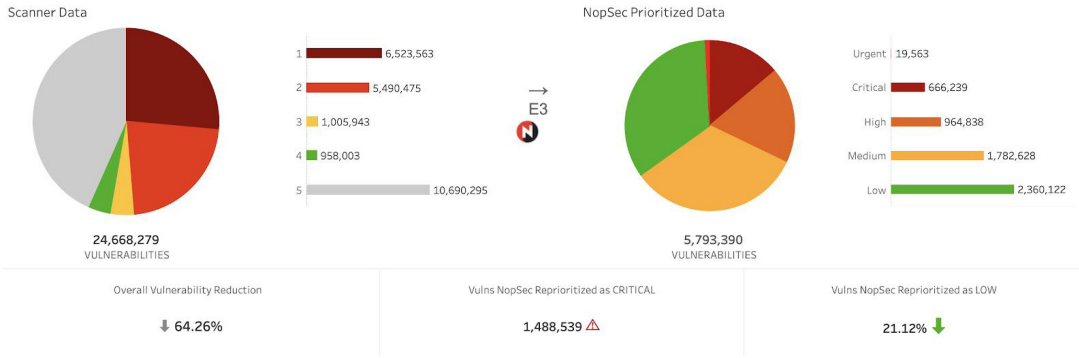
Threat Risk

The numbers are dropping as you go from non-threat vulnerabilities to active threat to potential threat–vulnerabilities that do not have a real present connection to threats but that have characteristics of similar vulnerabilities that do.

Prioritizing vulnerabilities is important to focusing on vulnerabilities that are mostly and currently under attacks on assets that matter the most to your organization. When those attacks are no longer correlated to those vulnerabilities, the overall related risk decreases over time.

Also, threat-based prioritization helps reduce the remediation effort to the vulnerabilities that matter the most in your environment.

THREAT-BASED PRIORITIZATION

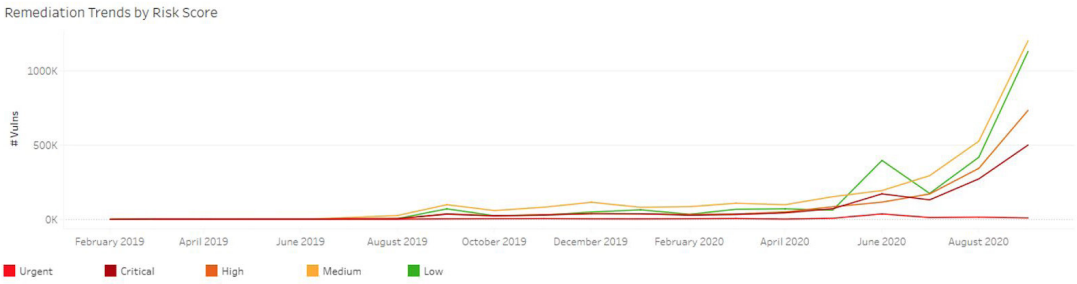


NopSec's risk prioritization engine helps achieve an overall vulnerability reduction prioritized by almost 60%, with 1.2 million vulnerabilities reprioritized as critical and an overall 22.6% vulnerabilities deprioritized as Low risk.

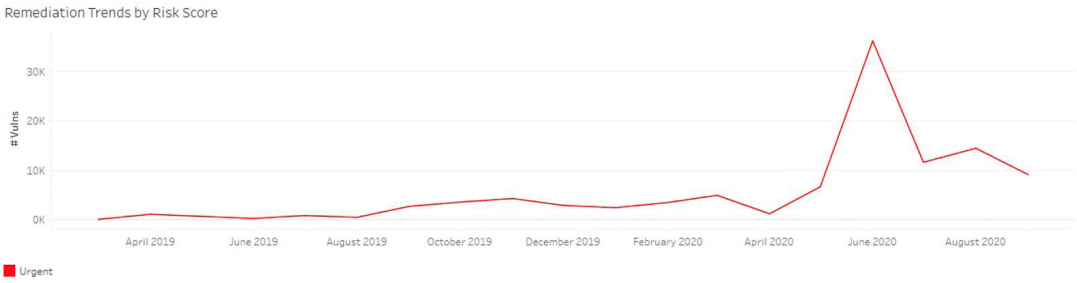
Most importantly, the prioritization's net effect is to increase the total number medium and low vulnerabilities, slightly increasing the critical and high risk categories, and introducing the Urgent category of risk for an extremely targeted remediation effort.

REMEDIATION AND PATCH MANAGEMENT

On vulnerability management remediation trends, the chart below describes the number of closed vulnerabilities by patching and workaround across time. An expected “hockey-stick” trend is depicted, showing organizations that increase their vulnerability management maturity over time.

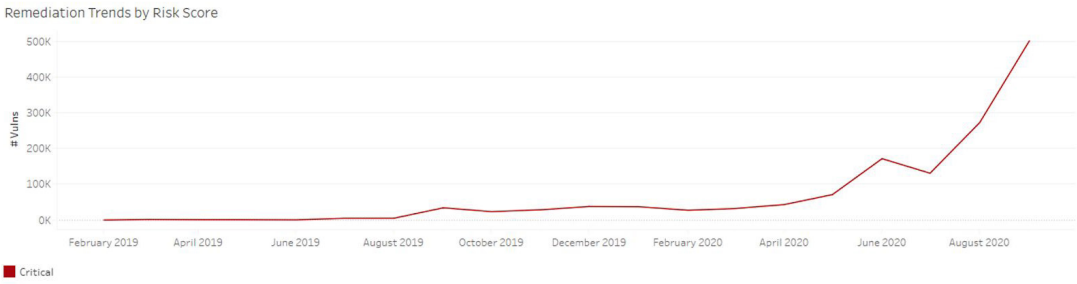


More interesting is to see how Urgent and Critical vulnerabilities have been closed through remediation.



Urgent vulnerabilities have been closed in the thousands with some peaking in the tens of thousands. The remediation trend is pretty steady indicating that the organizations are closing vulnerabilities that are associated with threats and real targeted attacks at a higher pace than in the past. In remediation, showing an “urgency” label does matter!

The closing rate for critical vulnerabilities have been even higher with numbers in the hundreds of thousands collectively and trending upwards.



REMEDIATION AND PATCH MANAGEMENT

In terms of remediation and mean-time to remediation (MTTR), organizations do not seem to privilege quicker remediation performed on more critical vulnerabilities. Instead, organizations seem to choose a steady remediation speed across vulnerability risk categories, indicating that, besides for urgent vulnerabilities, in average vulnerabilities of any risk categories are remediated uniformly as part of a well formed vulnerability risk management program.

Patch Summary

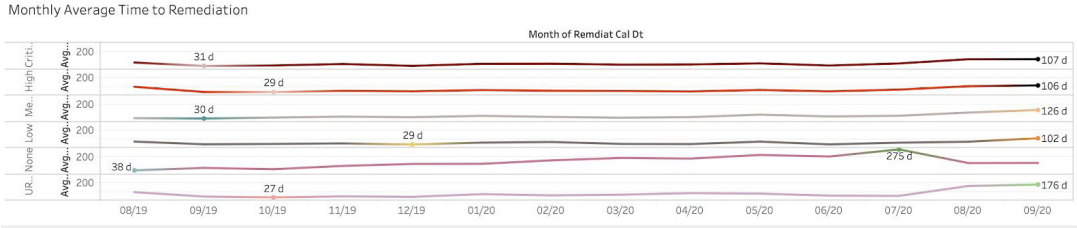
Anonymous Cln..	Vuln Risk	Avg. MTTR	
Banking Client 1	Low	67 days	54.81%
	None	34 days	12.90%
	Urgent	97 days	87.45%
Banking Client 2	Critical	113 days	86.76%
	High	109 days	88.40%
	Medium	174 days	72.58%
	Low	110 days	77.56%
	None	106 days	84.42%
	Urgent	138 days	95.67%
Banking Client 3	Critical	2 days	100.00%
	Medium	34 days	63.08%

For Urgent vulnerabilities, the related MTTR seems pretty high for such important vulnerabilities with the local government sector having longer MTTR, followed by media and banking sectors.

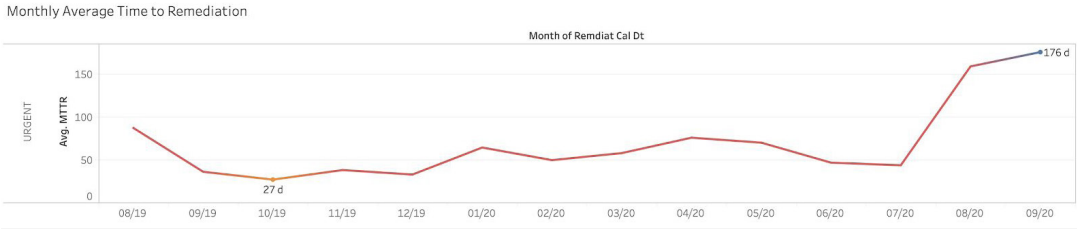
Patch Summary

Anonymous Clnt Nm	Vuln Risk	Avg. MTTR	
Banking Client 1	Urgent	97 days	87.45%
Banking Client 2	Urgent	138 days	95.67%
Banking Client 4	Urgent	27 days	89.93%
Banking Client 6	Urgent	178 days	100.00%
Banking Client 7	Urgent	62 days	93.75%
Computer Software Client..	Urgent	89 days	94.70%
Healthcare Client 1	Urgent	67 days	49.12%
Higher Education Client 1	Urgent	55 days	87.50%
IT Service Client 1	Urgent	75 days	81.03%
Local Government Client 1	Urgent	120 days	17.39%
Manufacturing-Durables	Urgent	39 days	99.48%

The chart below depicts the monthly average in vulnerability MTTR, showing an increase in the MTTR across all vulnerability risk categories which is greater than 100 days.

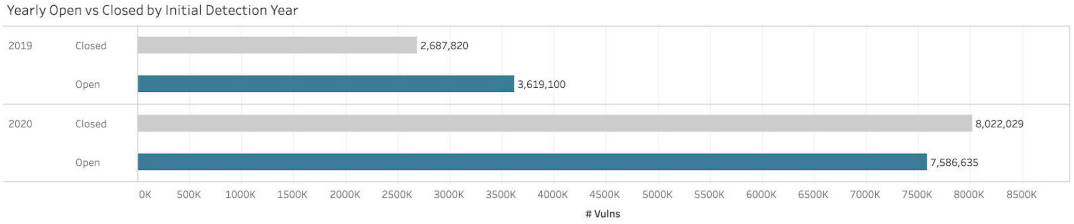


If you filter down the chart above to show only Urgent vulnerabilities, the same trend remains, going up to 176 days in September 2020.

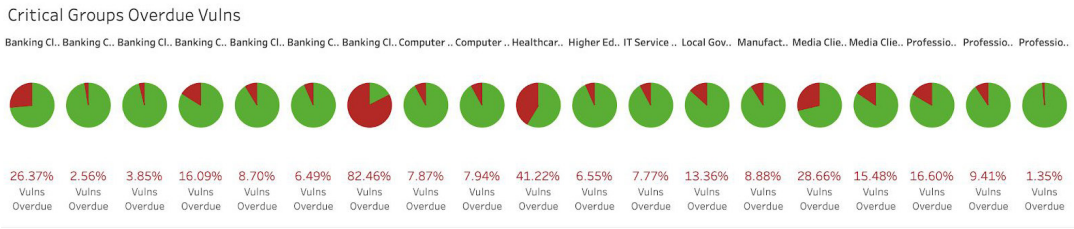


In terms of open and closed vulnerabilities by detection year, the year 2020 saw an overall increase in both vulnerability detection and remediation, compared to the year 2019, indicating that overall organizations are getting on with the vulnerability management plans, increasing their maturity and effectiveness in managing their programs.

REMEDIATION AND PATCH MANAGEMENT



In terms of meeting vulnerability remediation Service Level Agreements (SLAs), most of the customers meet most of their vulnerability SLAs with low number of vulnerability remediations overdue, barring few exceptions for healthcare and banking verticals.



The overdue SLAs are in the Critical, High and Medium vulnerability categories mostly in 45-60 days, 60-90 days and above 90 days time frame respectively. These three categories affect the Critical vulnerability risk. No Urgent vulnerabilities are shown as overdue, which reveals the urgency of the risk has a deep effect on the timing of the remediation.

LESSONS LEARNED

Remediation program management is often misunderstood as a centralized program with uniform processes, much like a jogger on a running track. Add more joggers, or hire faster joggers, and you'll fix more at the same time is the logical conclusion. If only this were true, more organizations would be safer faster. A more accurate analogy would be "The Hunger Games" race: in it there are unique problems with varying levels of value and you'll need different skill sets to solve them. Oh, and about those rules, attackers don't follow them. With all of these variables–and some of the uncontrollable–how do you know if you are getting better?

Successful customers have identified one quantitative measure to inform progress: SLAs. So how do you account for all of the complexity with just one number? By adding dimensions to the SLA. There are different SLAs for different classes of remediation. For example, assets that have critical business impact have a much tighter SLA than printers. Another dimension is driven by vulnerability classification. Vulnerabilities that can be exploited remotely in non-critical assets can still enable lateral movement when combined with local escalation privilege exploits. Multidimensional SLAs can normalize these real-risk scenarios to a single quantifiable number in order to track progress. The best way to identify which dimensions should be utilized depends on the organization's overall goal in vulnerability management.

THE VULNERABILITY LANDSCAPE BASED ON NOPSEC CLIENT DATA

The following are trending considerations based on the most frequent vulnerabilities found in NopSec clients vulnerability management programs.

It is important to understand the vulnerability landscape of the trending vulnerability in a population to understand risk posture and how the vulnerability risk management program fits in the risk management strategy.

These are the top 20 most frequently found vulnerabilities across all NopSec clients. A number of interesting insights can be gleaned from this top 20 list and are mentioned following the list.

TOP 20 MOST FREQUENTLY FOUND VULNERABILITIES:

- CVE-2020-1035 - A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
- CVE-2020-1092 - A remote code execution vulnerability exists when Internet Explorer improperly accessed objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
- CVE-2020-1060 - A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
- CVE-2020-1093 - A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
- CVE-2020-1058 - A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
- CVE-2020-1062 - A remote code execution vulnerability exists when Internet Explorer improperly accessed objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
- CVE-2020-1064 - A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input. An attacker could execute arbitrary code in the context of the current user.
- CVE-2019-7832 - A Heap Overflow potentially leading to Arbitrary Code Execution.
- CVE-2020-0909 - A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.
- CVE-2020-1072 - An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the users system.

THE VULNERABILITY LANDSCAPE BASED ON NOPSEC CLIENT DATA

- CVE-2020-1048 - An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
- CVE-2020-1114 - An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
- CVE-2020-1154 - An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.
- CVE-2020-1078 - An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.
- CVE-2020-1153 - A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system.
- CVE-2020-1174 - A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'.
- CVE-2018-12126 - Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A potential security vulnerability in CPUs may allow information disclosure.
- CVE-2018-12127 - Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
- CVE-2018-12130 - Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
- CVE-2019-11091 - Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

Here is a quick analysis of the trending CVEs and which vulnerability types are the most recurring among our customers.

Most of these high risk vulnerabilities are remote code execution in the Windows environment or privilege escalation vulnerabilities to gain a more privileged user's access rights - except for low risk vulnerabilities that are still trending in customer environments. They enable the attacker to land and then expand into the organization's network. These one hit wonders are the most popular due to the ease of execution: they require exploiting a single vulnerability. These characteristics definitely expose the risk of executing code remotely or elevating user privileges in a highly distributed environment such as Windows. The only one denial of service vulnerabilities is an outlier of the trend expressed above. About 20% of the vulnerabilities reveal information through side-channel attacks. These attacks are useful if the host is also misconfigured, for example, if the passwords are not hashed or encrypted.

THE VULNERABILITY LANDSCAPE BASED ON NOPSEC CLIENT DATA

CVSS SCORE: IS IT ENOUGH?

Previously, we talked about vulnerability prioritization and how NopSec uses a threat-centric approach to vulnerability prioritization. In the following paragraphs we are going to explain how CVSS (Common Vulnerability Scoring System) works, the various versions of and differences between CVSS score versions and why CVSS vulnerability prioritization is not enough.

The CVSS score is the industry-standard way of assessing the severity of security vulnerabilities.

The CVSS score was designed to measure the technical severity of a vulnerability, but is widely misused as a means of vulnerability prioritization and assessing risk.
CVSS base score does not account for temporal evolution of a vulnerability (existence of exploits, malware, etc.) and asset context (asset value) and as such does not reflect the real risk posed by a vulnerability.

It is either not efficient or advisable to prioritize vulnerabilities based on CVSS score only, as it marks too many vulnerabilities as high or critical while scoring many of the truly dangerous ones as medium or low severity. In the 2018 State of vulnerability report, NopSec has extensively covered why CVSS v2 score is not enough by itself. This year, we would like to shed some light on the CVSS v3.1 score, highlighting the main differences between V2 and V3 of CVSS score and why the CVSS score version 3 is still not a complete measure for vulnerability prioritization.

Authors of CVSSv3 worked to introduce scoring changes that more accurately reflected the reality of vulnerabilities encountered in the wild, compared to CVSSv2. The three major metric groups – Base, Temporal, and Environmental each remained the same, but with changes within both the Base and the Environmental groups.

In the Base group, several changes were made:

- Confidentiality, Integrity, and Availability metrics were each changed to have scoring parameters of None, Low, or High.
- The Attack Vector metric added the Physical (P) value, which indicates a vulnerability where the adversary must have physical access to a system in order to exploit the vulnerability.
- A new metric, User Interaction (UI), was added. This metric indicates whether or not the cooperation of a legitimate user is needed to conduct an exploit.
- Another new metric, Privileges Required (PR) was added to indicate that administrative or other escalated privileges on the target machine must be achieved in order to successfully exploit the system.

In the Environmental group, the biggest change was that the environmental metrics in v2 were completely replaced with what's known as a Modified Base Score. Essentially, each of the Base metrics may be modified by the organization to reflect differences between their situation and environment vs others.

The followings are also the differences in terms of risk score conversion to vulnerability severity levels comparing CVSSv2 and CVSSv3.

CVSS v2 Rating Scale:
Low – Base Score of 0.0 – 3.9
Medium – Base Score of 4.0 – 6.9
High – Base Score of 7.0 – 10.0

THE VULNERABILITY LANDSCAPE BASED ON NOPSEC CLIENT DATA

CVSS V3 Rating Scale:
Low – Base Score of 0.0 – 3.9
Medium – Base Score of 4.0 – 6.9
High – Base Score of 7.0 – 8.9
Critical – Base Score of 9.0 – 10.0

Even the CVSS v3 score does not incorporate the threat-centric prioritization that comes from information coming from threat intelligence feeds. And it is neither expected for a technical risk score to have this situational awareness.

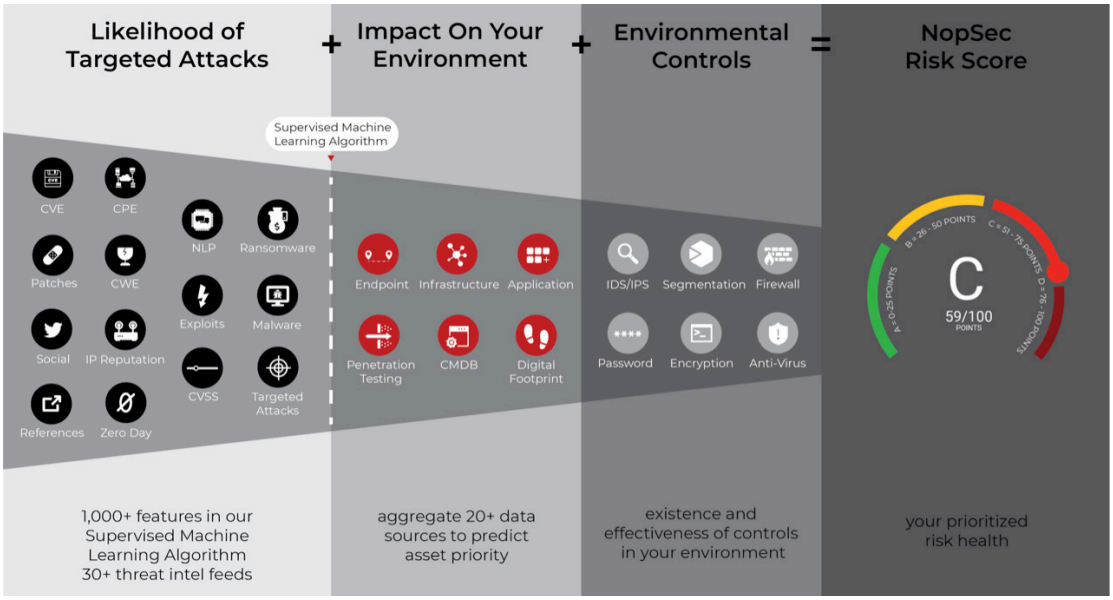
Industry standards, such as CVSS score, will not be enough for organizations to solve the cybersecurity problem. That is why the NopSec team drives further innovation that helps companies better manage their overwhelming cybersecurity challenges through creative solutions.

NopSec's ongoing mission is to help organizations improve their overall risk posture and to reduce the risk that is introduced by critical vulnerabilities actively being exploited today. One way that this is achieved is through vulnerability prioritization with Unified VRM. In an effort to increase focus on vulnerabilities with active exploits, and reduce the time it takes to remediate them, NopSec has updated the severity ratings in Unified VRM. Unified VRM features a new severity level called "Urgent", which prioritizes vulnerabilities that pose the highest immediate risk.

SEVERITY LEVELS AND THE NOPSEC RISK SCORE

In this section, we are going to look at how NopSec calculates its vulnerability prioritization risk score and the components of it which makes it so unique.

With its proprietary machine learning and daily ingestion of threat intelligence feeds, NopSec Unified VRM platform removes the manual analysis that goes into deciding which vulnerabilities to remediate. The NopSec Risk Score is calculated by looking at the likelihood of targeted attacks, the impact on the IT environment, and the risk reduction provided by compensating controls. After this calculation, each detected vulnerability ingested by Unified VRM ends up with a NopSec Risk Score between 0 and 100. The numerical Risk Score corresponds to a severity rating (Critical, High, Medium, Low) and Risk Grade (A, B, C, D).



THE VULNERABILITY LANDSCAPE BASED ON NOPSEC CLIENT DATA

One of the benefits of NopSec's machine learning scoring algorithm is to determine if a detected vulnerability is associated with any active threat (Malware, Ransomware, Trojan, Exploit Kit, or Targeted Attack). Active threats are attack vectors that are currently being used in the wild today by attackers. Visibility into this information is provided in Unified VRM through the Vulnerability Instance Description and with InstantSearch where threat has a "true" value. A lot of threat intelligence, social media, vulnerabilities and product vendor feeds contribute to this determination, as well the value of the assets and mitigating controls present in the environment.

THE URGENT SEVERITY LEVEL

Here in this section, we look at why NopSec introduces the new "Urgent" security level and all the differences in score that it introduces.
The new Urgent severity level represents a severity level for vulnerabilities that have the following attributes:

- NopSec Risk Score = 100
- Active Threat = True
- Risk Grade = D

VULNERABILITY COUNTS: BEFORE AND AFTER

When comparing the vulnerability counts before and after the addition of the Urgent category, there is a 1:1 relationship between vulnerability counts for High, Medium, Low and None vulnerabilities. The vulnerability counts for these severity levels will not be impacted. The number of vulnerabilities in the original Critical group will be equal to the sum of the vulnerabilities in the new Urgent and Critical groups. For example, if there were 1,000 vulnerabilities in the Critical group before the addition of Urgent group, then there are going to be 1,000 vulnerabilities in the new Urgent and Critical group combined (e.g. 150 Urgent + 850 Critical vulnerabilities).

CONCLUSION AND LESSONS LEARNED

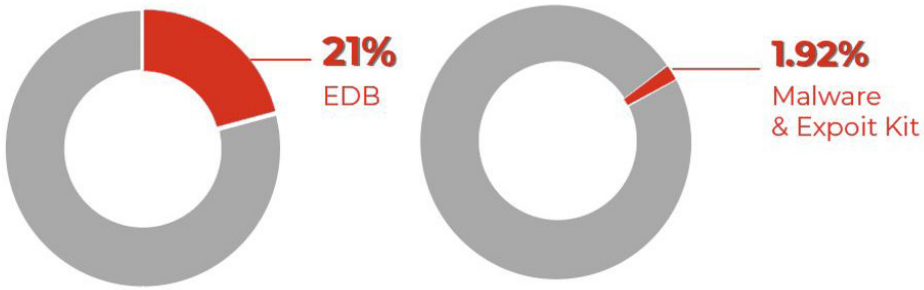
By calculating time-series totals across different vulnerability management key performance indicators and phases, this vulnerability management report teaches us an important lesson about the overall vulnerability management programs and their development. It is not that important where you are in your program in terms of maturity. What is important is the pace and the continuity of effort in improving it.

Proactive organizations - such as NopSec customers - choose to continue prioritizing remedial actions to the assets that matter the most to them, indicating the importance of an automated asset value prioritization. Remedial actions are needed the most where the most asset value is concentrated and where the attackers could strike with most frequency.

From the vulnerability assessment standpoint, despite what it was believed in the past, it is not that important the number of vulnerabilities detected in an organization's networks and applications. More important is the continuity of vulnerability scanning and the depth of detection, with preference to authenticated and agent-based vulnerability scanning, which are less false positive prone.

For the purpose of reducing the huge number of vulnerabilities detected, threat-based vulnerability management is nowadays essential to make the overall program manageable and focusing where the attackers pose the most risk. As past NopSec research shows (2018 State of Vulnerability Report), most of the targeted attacks and malware use a small number of vulnerabilities (~2% of the overall detected vulnerabilities) which can be found in both the critical and medium/low scale of the CVSS score ranking. Vulnerability correlation with a present threat and targeted attack is important. It is also important to understand the vulnerability characteristics to predict those vulnerabilities that would have exploits and targeted attacks in the near future.

In the 2018 State of Vulnerability Report, NopSec found that approximately 21% of CVEs published have associated exploit code in the Exploit Database alone. However, only 1.6% have associated Metasploit modules. Less than 2% (1.92%) have been linked to malware and targeted attacks. Roughly 95% of vulnerabilities ranked as high have never been linked to malware seen in the wild.

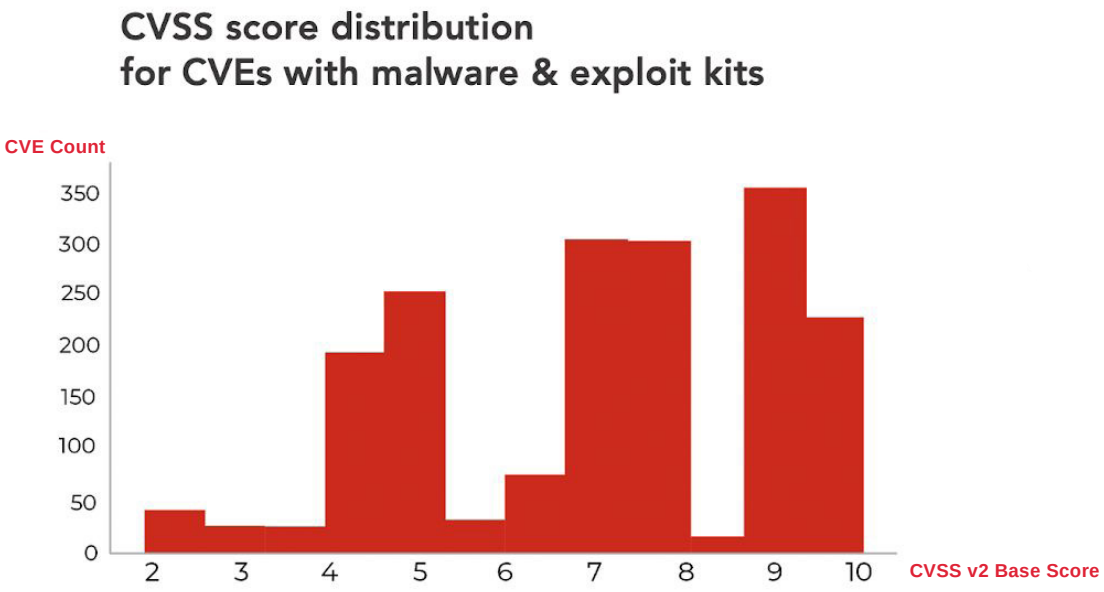


Also, as shown in the 2018 State of Vulnerability Report and in the chart below, vulnerabilities with malware and targeted attacks can also be found in the medium risk category; therefore, only fixing high and critical risk vulnerabilities creates a false negative problem.

CONCLUSION AND LESSONS LEARNED

NopSec found that:

- ~44% of CVEs with historical or recent malware & exploit kit association have CVSS base score <7 – medium or low severity.
- If you only prioritize based on high CVSS score, you are likely to miss many dangerous vulnerabilities – CVSS score alone likely to lead to many false negatives as well (CVEs that do have malware / targeted attack association, but wouldn't be picked up as such).



Vulnerability remediation has been showing encouraging trends lately with organizations seeking value-for-money for their vulnerability risk management programs. Focusing on urgent and threat-based vulnerabilities trying to remediate 100% of them at once with very low MTTR has decreased significantly the overall threat risk organizations are facing over time.

In terms of prioritization, we recently had an interesting case where for the urgent "Zerologon" vulnerability (CVE-2020-1472) the vulnerability bulletin was almost ignored - or not prioritized - at first by the leading infrastructure vulnerability scanning vendors. The reason for this lack of prioritization was because there were no details and there were no public exploits back when the first vulnerability details emerged. That started to change dramatically when the full review by Secura was published.

This case highlights how important it is to have a capable ML algorithm that prioritizes vulnerabilities above and beyond the ones that have malware and targeted attacks correlation today. The Secura analysis revealed later that the Zerologon was indeed an unauthenticated remote code execution, and not a privilege escalation like it was first identified as.

An ML algorithm - such as NopSec's - that identified early on an urgent vulnerability by its description language as "super" important to be remediated with priority and independently from the present correlation with targeted attacks and exploits is essential to have a proactive vulnerability management program to fix vulnerabilities that might turn out to be very risky for the organization's networks and application security.

CONCLUSION AND LESSONS LEARNED

Security patching is indeed only one facet of the possible risk remediation strategies. The others - workarounds and mitigating controls - are as effective and often the only remediation strategies available under certain circumstances.

Furthermore, organizations still need to work on improving meeting their SLAs vulnerability MTTR in the critical and high risk vulnerability categories.

In terms of overall vulnerability management programs, more automation and not more people added to the VM program is needed to improve the overall program's efficiency and effectiveness.

The next frontier of vulnerability risk management is what differentiates each organization in its response to emerging threats against their environment and their customer's data: their control environment. Each organization puts forward its best threat and vulnerability management program which also includes "mitigating controls" - such as firewall rules, network segmentation, endpoint security solutions, and more. The mitigating controls are the front line of defense against those very vulnerabilities exploitation found on networks and applications. Those are the real differentiators among organizations putting their defenses up against threats and attackers out there. Therefore, it is important to incorporate the mitigating controls as a decreasing effect of the overall vulnerability risk score since they are there to mitigate the risk that a successful exploitation takes place.

About NOPSEC

NopSec offers its flagship product, Unified VRM® (Vulnerability Risk Management), a cloud-based SaaS platform that helps organizations proactively manage vulnerability risk lifecycle from inventory, detection, prioritization, remediation, validation to overall program governance and reporting.

The company is based in New York City. www.nopsec.com

2020 STATE OF VULNERABILITY MANAGEMENT REPORT