SIXGILL WHITE PAPER

Prioritizing CVEs: A New Approach to an Old Problem

April 10, 2019

Prioritizing CVEs: A New Approach to an Old Problem

CVEs (Common Vulnerabilities and Exposures) are lists of publicly available vulnerabilities and exposures related to software and hardware. Their purpose is to facilitate the sharing of data and to alert users of required actions to mitigate potential threats in the cyber world.

Nowadays, CVE identification and prioritization have become a prominent part of every vulnerability management tool, and an integral component in any risk assessment.

Most organizations rely on CVE feeds for their day-to-day cyber-defense operations. Those feeds -- although valuable to the users -- suffer from several major flaws, which unnecessarily expose users to cyber-attacks:

- **Failure to Handle the Explosion of Data** - The number of CVEs is sky-rocketing, with 15,000 CVEs in 2017 alone. Thus, organizations face a hard time in prioritizing the CVEs to be fixed and are struggling to patch outdated CVEs.

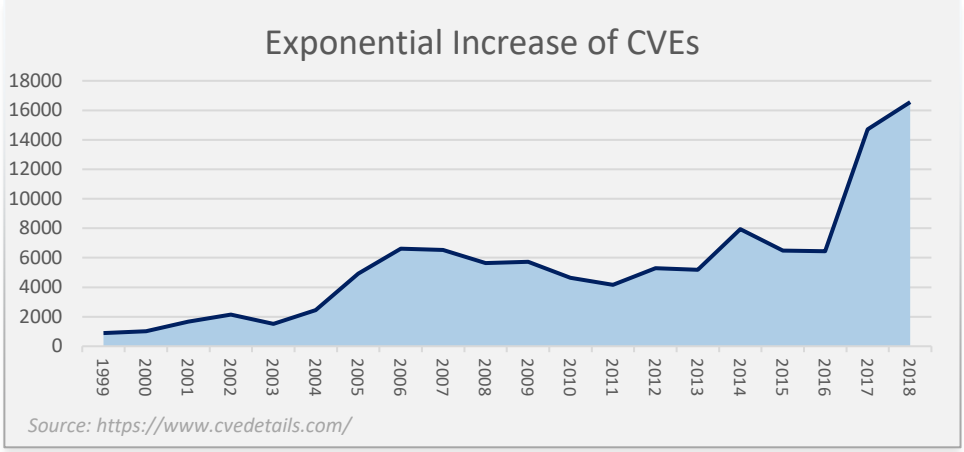


Figure 1: The number of CVEs is increasing exponentially by the year, exceeding 15,000 CVEs published per year.

- **Failure to Handle New CVEs in a Timely Manner** – In most cases, other solutions use manual calculation to identify and prioritize the handling of new CVEs. This approach is time-wasting, resulting in the fact that some CVEs wait for weeks to be analyzed. That crucial space of time leaves the door open for threat actors to exploit the vulnerability, while organizations are unable defend themselves.

Figure 2: CVE-2013-2094 and CVE-2016-5195 are still used in late 2018 in new trojans and malwares.

- **Failure to Take into Consideration Outdated CVEs** - Current solutions focus on recently discovered CVEs, but fail to address threats posed by "old" CVEs. These older CVEs may be even more severe and urgent to fix then the new ones. Threat actors understand this gap and look to exploit it.
- **Failure to Automatically Detect Customer Assets** - Current solutions require the customer to manually insert an exhausting list of assets to be monitored, risking an incomplete and flawed intelligence solution.
- **Failure to Calculate CVE Rating in a Dynamic Manner** – Current solutions analyze the CVEs based on a static rating which updates no more than 2-3 times in the CVE's lifecycle. This approach puts the customer at risk of operating on obsolete information and false assumptions.

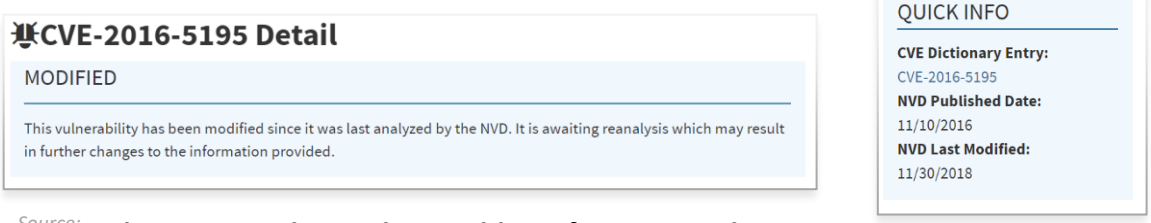


Figure 3: CVE-2016-5195, also known as "The Dirty Cow" Vulnerability, has "High Severity". Nevertheless, it is awaiting reanalysis for more than a month now, after its last revaluation was two years ago.

Source:

- **Failure to Look at the Problem from a Multi-Layer Perspective** - Current solutions offer a static rating for CVE severity, calculated based on the potential damage the CVE would cause if exploited. By choosing a one-dimensional approach, current solutions fail to consider the intent of the threat actors, thus overlooking the probability of the CVE to be exploited or not.

To overcome these acute problems, organizations must take a step forward in vulnerability assessment solutions and embrace an advanced approach that tackles the issue in an efficient, timely and accurate manner.

A New Approach: Integrating Exploit Probability with Impact Severity

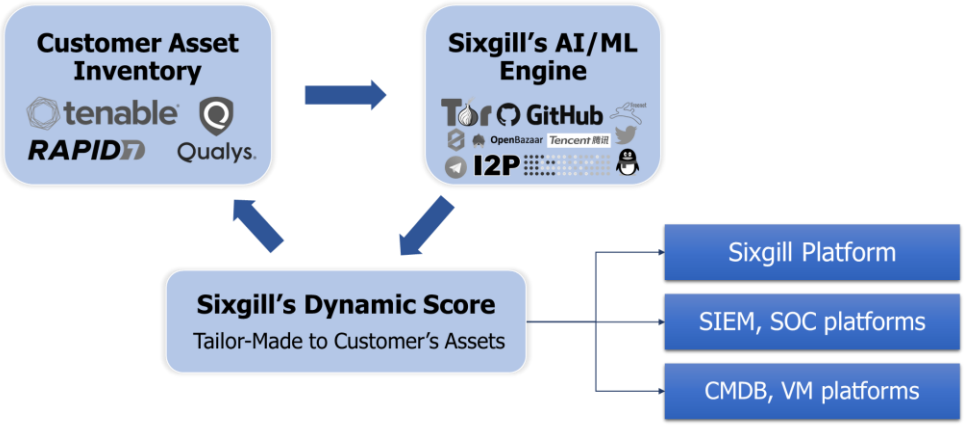
In light of current challenges, there is an urgent need for a complementary approach to handling CVEs. Such an approach should focus on a dynamic rating, derived from the underground discourse on deep and dark web forums. Combined with other sources -- such as code repositories and technical know-how – dynamic CVE rating will enable organizations to track threats from CVEs that most others define as irrelevant or obsolete, but have a higher probability of being exploited by threat actors.

Driven by the dynamic rating of the CVEs, an alert mechanism based on the customer's assets will allow organizations to take concrete, effective and timely measures to mitigate these threats.

Alerts should be based on an up-to-date list of relevant customer assets, automatically and autonomously fed by a continuous scan of the organization's assets and exposures.

By dynamically rating CVEs and alerting the customer of threats that are relevant to their specific assets, this approach will provide an end-to-end solution for CVE prioritization and remediation.

AN END-TO-END CVE PRIORITIZATION AND REMEDIATION SOLUTION – A SUGGESTED ARCHITECTURE



WHAT SHOULD A THREAT INTELLIGENCE PLATFORM CONSIDER WHEN CALCULATING EXPLOIT PROBABILITY?

Every CVE's severity score is determined by the National Vulnerability Database (NVD) in what is referred to as the Common Vulnerability Scoring System (CVSS). While the CVSS is a standard measurement system for vulnerability impact scores, it does not encapsulate the full spectrum of risk posed to the client's assets.

Our suggested approach offers a new score – the CVE Exploit Probability score, to be calculated based on several parameters:

- **When was the CVE published?** CVEs which were published more recently will have a higher probability of being exploited by threat actors
- **Does the CVE have a proof-of-concept exploit code on GitHub?** Threat actors are lurking for POC exploit codes in code repositories such as GitHub, waiting for an opportunity to use them as part of their malicious campaigns.

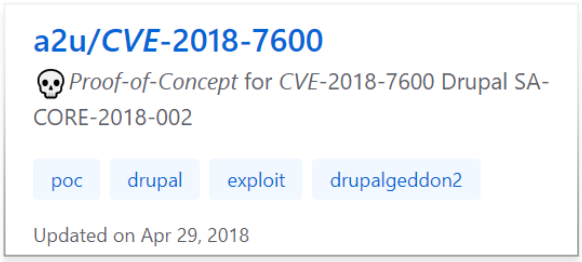


Figure 4: Proof of Concept exploit code for CVE-2018-7600, as shared on GitHub, a month after the CVE was published by

- **Does the CVE have a proof-of-concept exploit code offered on Dark Web forums?** Exploit codes are also bought and sold on dedicated markets on the Dark Web, allowing less sophisticated actors to execute advanced attacks.

Figure 5: A threat actor published a manual for exploiting CVE-2018-15982 on the Chinese Deep Web

- **Was the CVE discussed on the underground?** CVEs that are the subject of discussions on the Deep and Dark web are more likely to be exploited by threat actors. The volume of discussion about the CVE and how recently these discussions took place are key factors in determining the exploit probability of the CVE.

Figure 6: Mentions of CVE-2015-5622 on the underground since 2015, as seen on the Sixgill platform. Although NVD defined CVE-2015-5622 as "not severe", we can clearly see threat actors' active interest in this vulnerability.

FROM WHICH SOURCES SHOULD A THREAT INTELLIGENCE PLATFORM COLLECT INFORMATION?

- **Underground Forums** –Deep, Dark and Surface Web forums are key places where threat actors discuss recent vulnerabilities, share exploit code and even plan joint attack campaigns using these exploits. To effectively prioritize intelligence from these sources, organizations need a solution that automatically extracts large amounts of information and analyzes it in a short period of time.

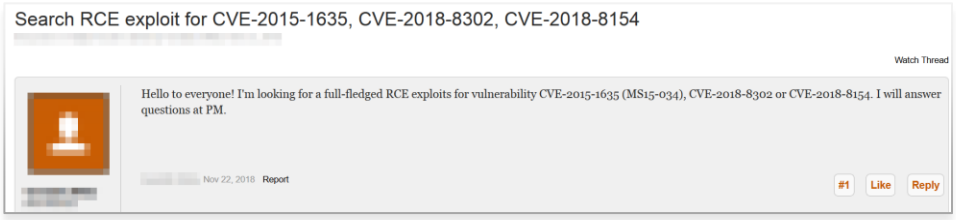
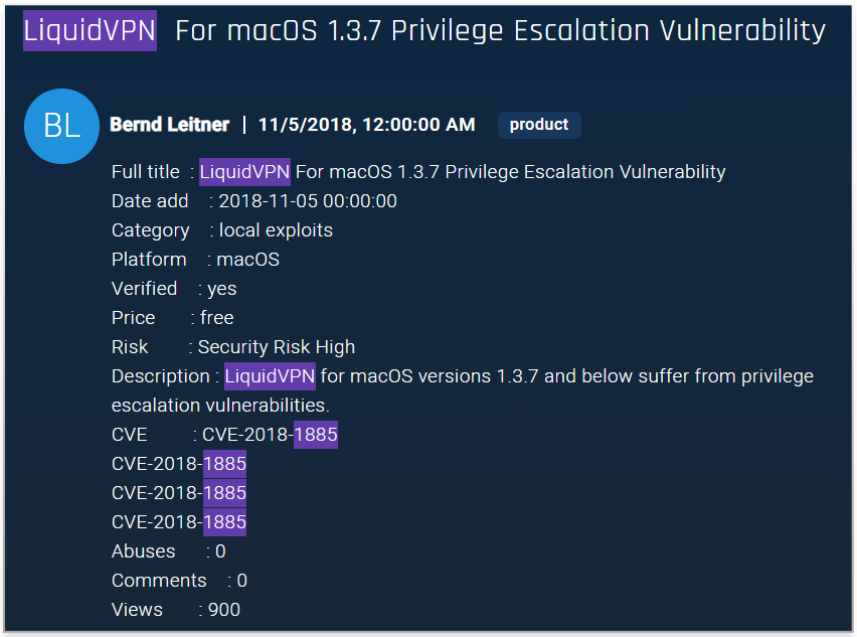


Figure 7: A threat actor is looking for exploit codes for several CVEs on a prominent Dark Web forum

- **Underground Markets** – Marketplaces on the Dark Web are used as a meeting place for buyers and sellers of exploit codes kits, Metasploits and other malicious tools. Thus, extracting information from this illicit trading platform and converting this information into structured data should play a prominent role in any CTI solution looking to solve the CVE prioritization challenge.

Figure 8: A threat actor offers an exploit code for CVE-2018-1885 on a Dark Web market, as seen on the Sixgill Platform



- **Code Repositories** – Proof-of-concept (POC) exploit codes are published daily on GitHub "for educational purposes only." Threat actors lie in wait for such golden opportunities, and every such POC code attracts significant interest from the malicious actors who look to exploit them.
- **Social Media** – Many users on Twitter, Telegram and other social media platforms share links to POC exploit codes, and updates regarding CVE exploitability trends. Tracking the discourse on these platforms provides early warning on new exploits and vulnerabilities.

Figure 9: A Twitter account shares a link to an exploit code on GitHub. The code is exploiting CVE-2018-11759

- **Paste Sites** – Threat actors share large chunks of text in these sites, which on some occasions include golden nuggets such as Metasploits, exploit codes and references to various CVEs.
- **Blogs, Cyber-Security Websites and Technical Feeds** – These sources provide indications that a CVE was used as part of an attack ("a weaponized CVE"), thus increasing the probability of the CVE being exploited again.
- **External Scanners** – In order for the threat intelligence platform to trigger customized alerts for the customer, any solution should scan the customer's network, reveal vulnerable products and correlate between the customer's assets and the dangerous CVEs that are relevant to them.

ABOUT SIXGILL

A market leader in deep and dark web cyber threat intelligence, Sixgill provides threat intelligence solutions to enterprises around the world, including Fortune 500 companies, financial institutions, and law enforcement agencies, addressing a wide range of cybersecurity challenges.

Our cyber threat intelligence solution focuses on our clients' intelligence needs, helping them mitigate risk to their organization, more effectively and more efficiently. Using an agile and automatic collection methodology, Sixgill provides broad coverage of exclusive-access deep and dark web sources, as well as relevant surface web sources. Sixgill utilizes artificial intelligence and machine learning to automate the production cycle of cyber intelligence, from monitoring, through extraction to production, uniquely focusing on relevant threats operating in these sources. For more information, visit: www.cybersixgill.com