Secureworks®

WHITE PAPER

Prioritizing Network Vulnerabilities:

A Survey and Comparison of Today's Options

Introduction

Remediating all vulnerabilities on a typical enterprise network is practically impossible. They often number in the thousands, tens of thousands, or even millions, and the list expands daily (more vulnerabilities were disclosed in the first quarter of 2019 than in any previous quarter). And like any software upgrade process, patching vulnerabilities carries risk, as an ostensibly innocuous patch could break something unintentionally. As much as remediating every identified vulnerability is an admirable goal, it is unrealistic for most enterprises, begging the question: which ones should be remediated first, and which should be considered low risk, and therefore low priority?

Today, there are three methods in use by which Security and IT teams can prioritize their vulnerabilities:

- CVSS (used as a risk rating)

- Predictive Exploitability

- Contextual Prioritization

This paper will provide a short overview of each, and provide an example of how each would score an actual vulnerability in the wild.

CVSS Score

Until recently, the CVSS score had been the only generally-available tool to segment vulnerabilities into risk categories. It's based on 6 factors specific to each vulnerability that hypothesizes a potential exploit and the risk the hypothetical exploit would pose. Using the standard risk model (likelihood of an occurrence combined with the consequence of that occurrence)

Likelihood	
Access	Can the vulnerability be exploited remotely or is physical access required?
Attack Complexity	Is the vulnerability easily exploited or does it require a degree of sophistication
Authentication	How many times an attacker would need to authenticate to exploit the vulnerability?

3 of the six factors address the likelihood of a successful compromise, while the other 3 address the impact of a breach exploiting the vulnerability.

Impact	
Confidentiality	Can the exploit lead to data theft?
Integrity	Can the data be compromised as a result of this vulnerability's exploitation?
Availability	Can the vulnerability expose the system to DDOS attacks or other threats to system availability?

All aspects of the CVSS score are public, including how the 6 factors are used to calculate the final score on a scale of 0 to 10 (10 indicating the most critical vulnerability level).

A combination of low predictability/repeatability, poor granularity, no accounting for web vulnerabilities, and its one-score-fits-all-organizations methodology makes it a poor choice for enterprises with more than a handful of assets.

Predictive Exploitability

While the CVSS score presumes a hypothetical exploit for each vulnerability, Predictive Exploitability attempts to predict the likelihood an exploit will be available at some point in the future for a newly discovered vulnerability. And if such an exploit is developed, how serious would its impact be (mirroring, again, the time-worn likelihood/consequence risk model discussed previously). Using machine learning, the technique attempts to classify each new vulnerability into existing categories, and then use that and other factors, to predict if an exploit for it will be developed and become available. Vendors promoting this technique have alleged high prediction accuracy rates, some claiming an over 80% ability to predict if a new vulnerability will result in an eventual exploit.

Contextual Prioritization

The newest vulnerability prioritization technique, Contextual Prioritization, is built on the premise that a vulnerability's risk is dependent not only on external factors that remain constant from enterprise to enterprise, but also on the unique environment of the vulnerability in the context of the network on which it resides. Leveraging machine learning and other AI technology at scale, Contextual Prioritization combines most of the characteristics of predictive exploitability about the existence - and likelihood of the eventual existence - of an exploit with over a dozen internal factors (e.g. is the asset with the vulnerability on an isolated subnet) to build a comprehensive risk score for each vulnerability.

Despite its widespread use, the CVSS score is inadequate as a primary vulnerability prioritization mechanism for most organizations.

Contextual prioritization doesn't assume that an existing or predicted exploit is enough to vault a vulnerability to the top of the priority list; an existing exploit is only one of nearly 3 dozen factors that yield a holistic view of the vulnerability's risk, a risk unique to each enterprise...and each asset in that enterprise with that vulnerability.

Comparing the 3 Approaches

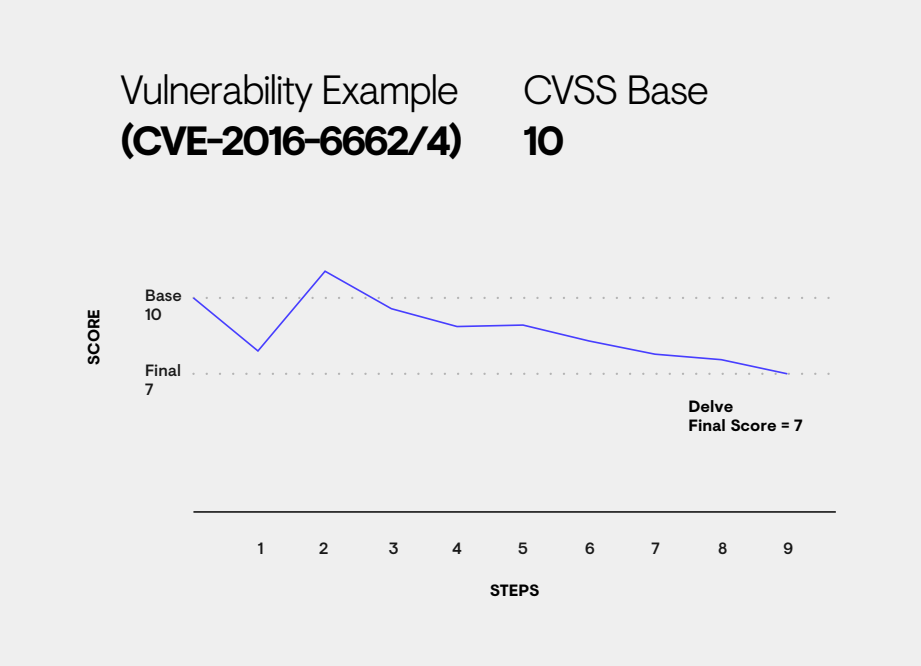
Perhaps the best way to appreciate each prioritization technique is to select a specific vulnerability and review how each method one would score it. We've selected CVE-2016 - 6662/4, a SQL-injection vulnerability discovered in 2016. The CVSS score for the vulnerability is 9.8, a combination of a 5.9 Impact Score and a 3.9 Exploitability Score. As for Predictive Exploitability, since an exploit for the vulnerability exists and the potential impact of this exploit could be significant, the Predictive Exploitability score for CVE-2016 - 6662/4 would be very high/critical as well.

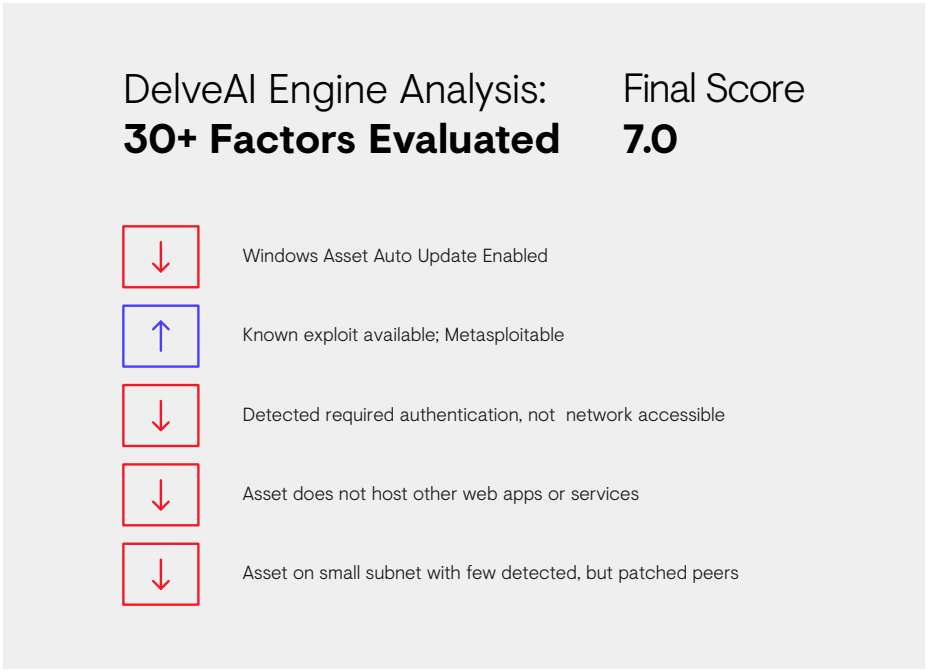
9.8

is the CVSS score for the vulnerability, a combination of a 5.9 Impact Score and a 3.9 Exploitability Score.

The Contextual Prioritization score, however, is less straightforward. In an analysis taken directly from an actual (anonymized) enterprise, multiple internal factors combine to actually lower the risk score of this vulnerability for this specific enterprise and this specific asset in that enterprise. The figure below illustrates how the Contextual Prioritization technique starts with the CVSS score and adjusts the score based on, in this case, 5 relevant risk factors (out of a possible 30+ factors considered overall). Some risk factors - like the existence of an existing exploit - increase the vulnerability's risk, while others decrease its priority.

It's important to emphasize that this analysis for this vulnerability is unique to the network environment of the enterprise this data was pulled from, and would be different - higher or lower - for a different enterprise environment. Indeed, the risk score of this vulnerability could be different for a different asset in another part of this same enterprise's network.





Caption: Accounting for the unique nature of a company's network environment can materially change the risk of a given vulnerability to an organization's information security.

The table below compares the risk factors considered by each technique when constructing their respective risk scores, and how those different analyses would result in significantly different risk scores for this vulnerability on this specific enterprise's network.

Risk Factor	CVSS	Predictive Exploitability	Contextual Prioritization
Windows Asset Auto Update Enabled	✗	✗	✓
Known Exploit Available & Metaspolitable	✗	✓	✓
Detected Required Authorization; not Network Accessible	✗	✗	✓
Asset Does Not Host Other Web Apps or Services	✗	✗	✓
Asset on Small Subnet with Few Detected, but Patched Peers Final Risk Score	✗	✗	✓
Final Risk Score	**9.8**	**Critical**	**7**

Summary

As long as network and software complexity continues to climb, and the corresponding number of vulnerabilities mounts, enterprises will search for ways to filter the highest risk vulnerabilities from the thousands that confront them. Today's machine learning and other technologies afford modern IT and security teams tools that were unavailable only a short time ago, tools that can considerably reduce the number of vulnerabilities that require immediate attention from the limited resources at their disposal.

Secureworks®

Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs.

With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.
www.secureworks.com

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp