

QUANTIFYING THE ATTACKER'S FIRST-MOVER ADVANTAGE

CONTENTS

Executive Summary	3
Findings	3
Recommendations	3
Introduction	4
Quantifying the Attacker's First-Mover Advantage	4
Analysis	6
Vulnerability Data Set	6
Median Delta	6
Negative Delta	7
Noteworthy Deltas	8
Conclusion	9
Appendix	11
High-Level Data Breakdown	11
Methodology	12
Limitations	12
Broader Analysis	13
Standards and Conventions	14
About Tenable	14

I. EXECUTIVE SUMMARY

This report measures the difference in days between when an exploit for a vulnerability becomes publicly available (Time to Exploit Availability) and when a vulnerability is first assessed (Time to Assess).

A negative delta indicates that the attacker has an opportunity to exploit a vulnerability before the defender is even aware of the risk.

The sample set used for this analysis is based on the 50 most prevalent vulnerabilities from nearly 200,000 unique vulnerability assessment scans.

Findings:

7-day

Attackers have a median seven-day window of opportunity to exploit a vulnerability before a defender is even aware they are vulnerable.

76%

of analyzed vulnerabilities had a negative delta – meaning the attacker has the first-mover advantage.

34%

For 34 percent of the analyzed vulnerabilities, an exploit was available on the same day that the vulnerability was disclosed.

24%

A further point of concern is that 24 percent of analyzed vulnerabilities were being actively exploited by malware, ransomware or exploit kits in the wild.

75%

While improving the Time to Assess by 75 percent would result in a positive delta for 66 percent of the analyzed vulnerabilities, the rapid Time to Exploit Availability and its weaponization mean that defenders often begin on a back foot and are challenged to gain the lead in the first move.

Recommendations:

- Use continuous vulnerability assessments to effectively improve the Time to Assess – but this by itself cannot fully mitigate the resulting exposure gap.
- Vulnerabilities and exploits are discovered and published incessantly, and attacks and threats evolve at a rapid pace and can strike at any time. The objective of an effective vulnerability management program must be to quickly adapt and react to these changing circumstances. A start-stop or cyclical model falls short in achieving this objective, requiring instead a vulnerability management approach based on a continuous integration and delivery (CI/CD) model.
- Align operational processes to support rapid response and ad hoc remediation and mitigation requests outside of regular maintenance and patch windows.
- Focus remediation and prioritization efforts on vulnerabilities with publicly available exploits and those actively being targeted by malware, exploit kits and ransomware. This necessitates up-to-date situational awareness and threat context.

II. INTRODUCTION

This research report examines the difference in time between when a public exploit for a vulnerability is published and when users actively assess it. These two events represent the first move the attacker and defender make.

The premise of this paper is that this delta is an indicative metric in determining [Cyber Exposure](#). The sample set is based on the analysis of real-world vulnerability assessment data from nearly 200,000 unique vulnerability assessment scans. We selected the 50 most prevalent critical and high-severity vulnerabilities from this data set for this report.

A basic understanding of how vulnerabilities are researched, assessed and exploited is assumed.

III. QUANTIFYING THE ATTACKER'S FIRST-MOVER ADVANTAGE

Security professionals are engaged in a continuous arms race with threat actors. In relation to vulnerabilities, this arms race is between attackers' access to exploits and defenders' ability to assess, remediate and mitigate them. The attackers gain and maintain the advantage if they can stay at least one step ahead of the defender, resulting in a window of exposure. The race is never-ending and begins again with every new vulnerability discovered. The finish line keeps shifting, with the attacker setting the pace.

Figure 1 outlines attackers' and defenders' first moves after a vulnerability is disclosed.

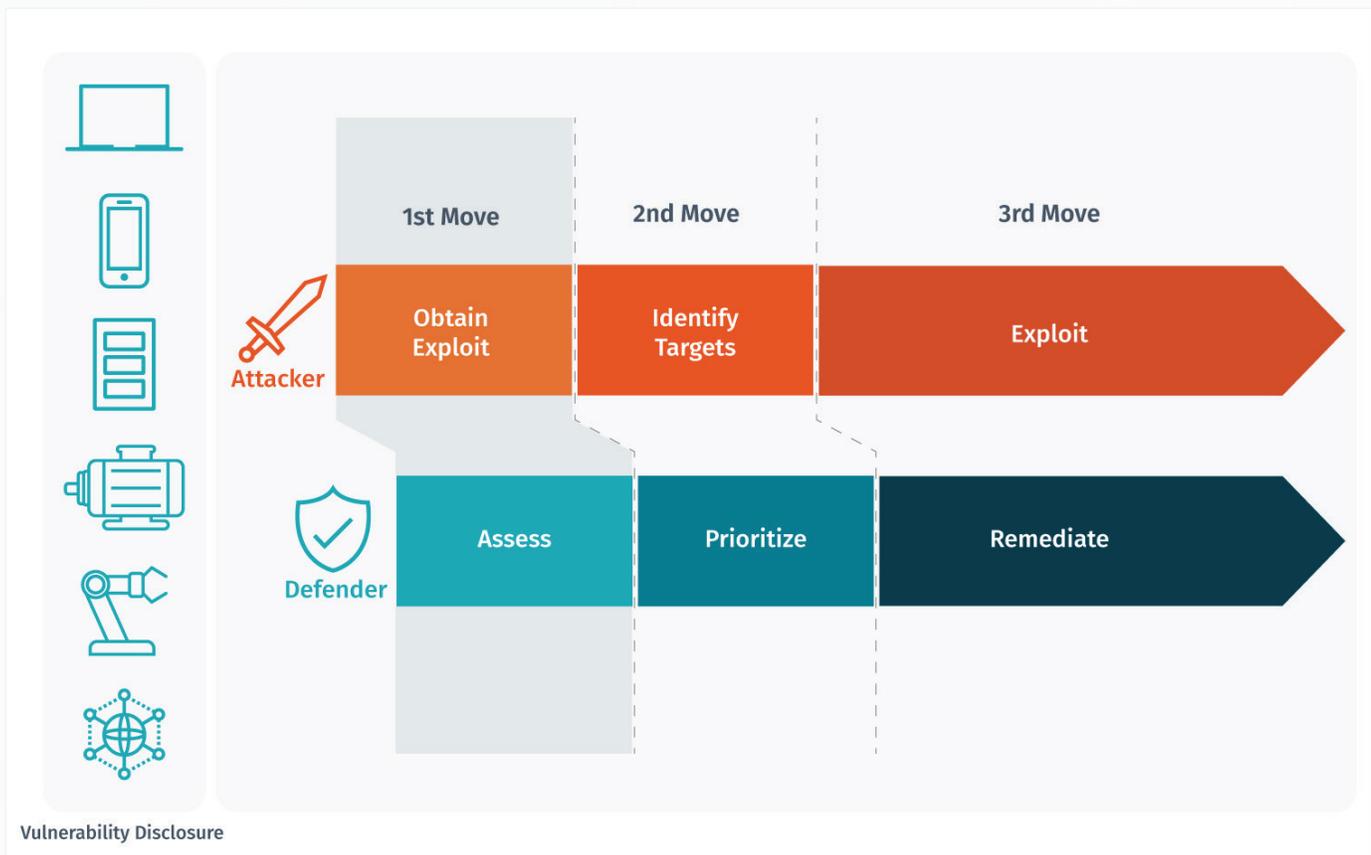


Figure 1. Attackers and Defenders First Moves Post-Vulnerability Disclosure

After a new vulnerability has been disclosed, the attacker's first move is to obtain a working exploit. For the defender, the first move is to assess whether the vulnerability impacts their organization and if they're at risk. The defender makes this assessment via a vulnerability scan. If we measure the Time to Exploit Availability (TtE) against the first Time to Assess (TtA), we will end up with a negative or positive number expressing the delta between the two:

- A negative delta indicates that the attacker has gained the first-mover advantage.
- A positive delta means that the defender has assessed the vulnerability faster than an exploit was available and has breathing room to initiate remediation and mitigation steps.

As long as the attacker retains the lead, the defender is exposed to risk, providing the attacker with a window of opportunity to strike with impunity.

In theory, the defender has time to remediate a vulnerability until an attacker actually exploits it. For most vulnerabilities, there is insufficient data available for when they are actively exploited in the wild. We do not always have the full view of what attackers are doing, so we must focus on what we can reliably determine and extrapolate from that information. When an exploit is available, we should assume it can and will be used. While other research has focused on TtE, this paper correlates TtE with TtA.

Our assumption for this analysis is that the race is a sprint, not a marathon. Measuring the attackers' and defenders' first moves provides insight into how the race begins and is a guiding indicator of how it will end. In other words, whoever seizes the lead with the first move typically retains the advantage. Leaving undisclosed zero-days aside, as soon as a public exploit is available, a vulnerability changes from a hypothetical to a real risk.

This analysis calculates the delta between the Time to Exploit Availability (TtE) and the Time to Assess (TtA) for the 50 most prevalent vulnerabilities by affected assets in the data set. The sample size is not sufficient to draw any broader conclusions about vulnerabilities. The delta will change depending on the prevalent vulnerabilities at any given time. For the delta calculated across a broader segment of vulnerabilities, please see the Appendix.

We are measuring the time difference between when an exploit is made publicly available and when the vulnerability is first assessed.

$$\Delta = TtE - TtA$$

TtE = Time to Exploit Availability

TtA = Time to Assess

IV. ANALYSIS

Vulnerability Data Set

To conduct the analysis and calculate the median delta, we generated our data set of vulnerabilities based on the following criteria:

- A severity of High (CVSSv2 7.0–8.9) and Critical (CVSSv2 9–10)
- A public exploit is available
- A Tenable plugin was released in 2017

We then selected the top 50 vulnerabilities based on the highest total of affected assets over a three-month period in late 2017. We used this selection criteria to ground the analysis in real-world activity.

V. MEDIAN DELTA

Median Delta	
Median Time to Exploit Availability (TtE)	5.5 days
Median Time to Assess (TtA)	12.8 days
Median Delta	-7.3

Table 1. Median Delta in 50 Most Prevalent Vulnerabilities

The results of the analysis of the most prevalent vulnerabilities showed that the median TtE across our sample set is 5.5 days. The median TtA is 12.8. This results in a median delta of -7.3. **This means that across the sample data set, the attackers have a median seven-day window of opportunity to exploit the vulnerabilities before the defender has even assessed for the vulnerability.**

Top 50 Most Prevalent Vulnerabilities Summary

Critical Severity

54% of the 50 most prevalent vulnerabilities are of Critical severity, with a CVSS version 2 Base Score of 9-10.

Exploited by Malware

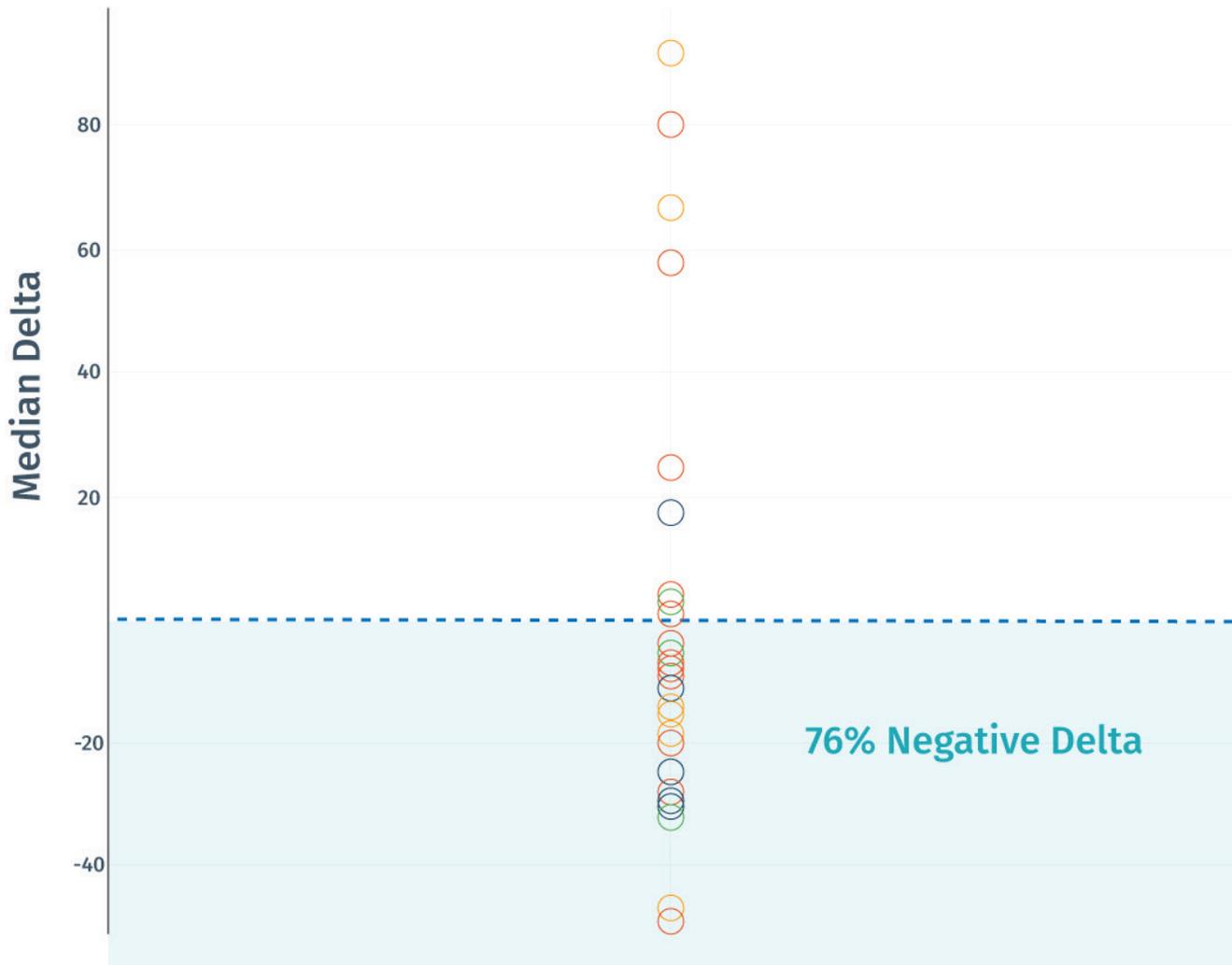
24% (12 out 50) of the included vulnerabilities are known to be targeted in the wild by malware.

In the News

14% (7 out 50) of the included vulnerabilities are considered High Profile by Tenable, based on coverage in the media.

Median Δ = **-7.3**

76 percent of analyzed vulnerabilities have a negative delta.



Negative Delta

For 76 percent of vulnerabilities, the delta was negative, meaning that the attackers gained the first-mover advantage. In 34 percent of cases, an exploit was made publicly available on the same day that a vulnerability was disclosed.

Worryingly, 24 percent of vulnerabilities in the data set were actively being targeted by malware in the wild, with a median delta of -6.7. Fourteen percent of vulnerabilities in the data are considered High Profile based on discussion in the media. These High Profile vulnerabilities have a median delta of -12.0.

Median “Exploited by Malware”

Delta: **-6.7**

Median “In the News” Delta: **-12.0**

Noteworthy Deltas

CVE	Name	Why Noteworthy?	Median TtE (in full days)	Median TtA (in full days)	Median Delta (in full days)
CVE-2017-5638*	Apache Struts Remote Code Execution Vulnerability	High Profile – root cause for Equifax breach	1	4	-3
CVE-2017-7494	Samba Remote Code Execution Vulnerability	High Profile and included in malware – SambaCry or Eternal Red. Related vulnerability to WannaCry but affecting Samba. Targeted by StorageCrypt Ransomware	0	9	-9
CVE-2017-8759	Microsoft Windows .NET Framework Remote Code Execution Vulnerability	High Profile and included in Malware – used by nation state APT groups to deploy FinSpy surveillance tool	1	7	-6
CVE-2017-5753** CVE-2017-5715	Multiple CPU Hardware Information Disclosure Vulnerability	High Profile – Spectre CPU vulnerability	0	15	-15

Table 2. Deltas for Noteworthy CVEs

*CVE-2017-5638, shown here for reference, was not present in the 50 most prevalent vulnerabilities, but was present in a larger sample data set. See the Appendix for details.

**Spectre was disclosed in early 2018, but was included for reference and comparison.

VI. CONCLUSION

Digital transformation has radically increased the number and types of new technologies and compute platforms – from cloud to IoT to operational technology – and led to a dramatic growth in the attack surface. Inevitably, this expanding attack surface has given rise to an unrelenting barrage of vulnerabilities. Yet, many organizations still run their operations programs on fixed cycles (e.g., every six weeks), which is inadequate in today's dynamic IT environment.

Latency is therefore built directly into the cybersecurity process, giving the attacker the advantage from the outset and creating a knowledge deficit. Many CISOs are left struggling to gain visibility into a constantly evolving threat landscape and are hampered in their efforts to proactively manage cyber risk based on business criticality.

Defenders are setting their pace based on internal factors, rather than on external drivers.

7-day

Attackers have a seven-day window of opportunity to exploit a vulnerability before a defender is even aware they are vulnerable.

76%

of analyzed vulnerabilities had a negative delta – meaning the attacker has the first-mover advantage.

In most cases where defenders manage to seize the advantage, it is because an exploit is made publicly available long after the vulnerability was disclosed, rather than a quicker TtA. Defenders aren't gaining first-mover advantage based on their own actions. The attacker is already racing around the first corner before the defender has even left the starting blocks. Defenders are acting like they are running solo, when they actually have an opponent.

The most effective way to retain a positive delta across the majority of vulnerabilities is to conduct continuous vulnerability assessments.

34%

For 34 percent of the analyzed vulnerabilities, an exploit was available on the same day that the vulnerability was disclosed.

75%

Improving TtA by 75% would result in a positive delta for 66% of the analyzed vulnerabilities.

Continuous vulnerability assessments are the best option given that TtA is dependent on plugin/signature availability and impacted by the overheads of vulnerability assessment at scale.

Based on the average time from vulnerability disclosure to exploit availability, improving the TtA by 60 percent would have still only resulted in a positive delta for 50 percent of the analyzed vulnerabilities. Improving the TtA by 75 percent would result in a positive delta for 66 percent of the analyzed vulnerabilities.

Our analysis of scanning behavior indicates that just over 25 percent of organizations are conducting vulnerability assessments with a frequency of two days or fewer. While this is an achievable goal, and will reduce the head start that attackers have for most vulnerabilities, it still leaves a negative delta and exposure gap for some vulnerabilities. This exposure gap can be decisive depending on the vulnerabilities in question.

With threat actors setting the pace, the remaining Cyber Exposure gap cannot be eliminated by a few tweaks or the security organization alone.

24%

of vulnerabilities in the data set are actively being targeted by malware in the wild.

14%

of vulnerabilities in the data are considered High Profile based on discussion and dissemination in the media.

With a negative delta across most vulnerabilities and vulnerability assessment generally lagging behind exploit availability, defenders must compensate in subsequent moves by improving their vulnerability management approach.

Effective vulnerability management programs can quickly adapt and react to the rapidly evolving threat landscape. Start-stop and cyclical models fall short. Instead, organizations need a vulnerability management approach based on a continuous integration and delivery (CI/CD) model.

This is not realistically achievable by the security organization alone. Rather, it necessitates better alignment with operational business units and the rest of the organization. To support this, operational processes must support rapid response and ad hoc remediation and mitigation requests outside of regular maintenance and patch windows.

Remediation and prioritization efforts must be focused on vulnerabilities with publicly available exploits and those actively being targeted by malware, exploit kits and ransomware. This necessitates up-to-date situational awareness and threat context to evaluate true risk and exposure as well as to inform and guide decision making.

Recommendations

- Use continuous vulnerability assessments to effectively improve the TtA – but this by itself cannot fully mitigate the resulting exposure gap.
- Vulnerabilities and exploits are discovered and published incessantly, and attacks and threats evolve at a rapid pace and can strike at any time. The objective of an effective vulnerability management program must be to quickly adapt and react to these changing circumstances. A start-stop or cyclical model falls short in achieving this objective, requiring instead a vulnerability management approach based on a continuous integration and delivery (CI/CD) model.
- Align operational processes to support rapid response and ad hoc remediation and mitigation requests outside of regular maintenance and patch windows.
- Focus remediation and prioritization efforts on vulnerabilities with publicly available exploits and those actively being targeted by malware, exploit kits and ransomware. This necessitates up-to-date situational awareness and threat context.

VII. APPENDIX

High-Level Data Breakdown

The breakdown below provides insight into the analyzed vulnerability data set. The sample set is insufficient to draw any broader conclusions and is not intended to be representative.

The table below lists the associated CPEs¹ for the analyzed vulnerabilities, in no particular order.

Operating Systems	Applications
Microsoft Windows	Adobe Flash Player
Red Hat Enterprise	Apache Struts
Apple MacOS	Apple Safari
Canonical Ubuntu Linux	Cisco WebEx
Novell SuSE Linux	Microsoft IE
Oracle Linux	Microsoft .NET Framework
CentOS Linux	Microsoft Malware Protection Engine
Oracle VM Server	Microsoft SharePoint
Debian Linux	Oracle VirtualBox

Table 3. CPEs Associated with Analyzed Vulnerabilities

1. Common Platform Enumeration, see: www.nvd.nist.gov/products/cpe

The table below shows a high-level breakdown of the metrics. The data clearly shows that outliers skewed the average.

Analysis of Outliers in Data Set	TtE	TtA	Delta
Highest Value in Data Set	145.0	50.2	116.6
Lowest Value in Data Set	0	5.9	-50.2
Average	15.0	17.1	-2.0
Median	5.5	12.8	-7.3

Table 4. Analysis of Outliers in Data Set

Methodology

Our analysis focuses on vulnerabilities that fulfilled the following criteria:

- A severity of Critical (CVSS2 7.0-8.9) and High (CVSS2 9.0-10)
- A public exploit is available
- A Tenable plugin was released in 2017
- The highest prevalence by affected asset count in Tenable.io assessments over a three-month period in late 2017

We based the prevalence on the total amount of affected assets in the specified time frame. Additionally, we considered the highest one-day peak for affected assets.

We measured the TtE based on the difference in days from the date that a vulnerability was publicly disclosed according to VulnDB² and the date that an exploit was made available on Exploit-DB³. There will always be cases where an exploit may have been made available earlier via a different channel, but for the purpose of this analysis, VulnDB and Exploit-DB were chosen to provide a standard benchmark.

We measured the TtA based on the VulnDB vulnerability disclosure date and the date that a relevant plugin was first included in a vulnerability scan.

Limitations

- Our vulnerability disclosure date was based on VulnDB vulnerability disclosure dates. There may be exceptions where a vulnerability was disclosed at an earlier date (e.g., on darknet).
- Our exploit availability date is derived from Exploit-DB. There may be cases where an exploit was publicly made available at an earlier date, for example via zero-day exploitation.
- Exploit availability does not necessarily mean active exploitation. Usually, only a subset of exploitable vulnerabilities are, for example, weaponized and automated in the form of malware, ransomware and exploit kits. A human threat actor, however, would have access to any published exploit.
- The sample set size of 50 vulnerabilities is not representative and is insufficient to draw detailed or broader conclusions about vulnerabilities in general.

2. VulnDb is a proprietary vulnerability database from Risk Based Security; 3. Exploit-DB is maintained by Offensive Security

Broader Analysis

Tenable Research previously conducted a delta analysis based on a sample set of 430 unique CVEs.

The criteria for the sample set was:

- Vulnerability was published in 2017
- A public exploit was available
- A sufficient prevalence to permit a representative TtA calculation

Compared to the most prevalent exploitable vulnerabilities, the delta varied, but the overall trend is still negative. The table below shows the metrics for both data sets:

	2017 Exploitable Vulnerabilities	50 Most Prevalent Vulnerabilities
Median TtE (in days)	7.1	5.5
Median TtA (in days)	11.8	12.8
Delta = TtE - TtA	-4.7	-7.3

Table 5. Comparison of Median Deltas in Two Data Sets

Standards and Conventions

Throughout this report, we refer to specific terms as defined below:

Term	Definition
Exploit Availability	The date that an exploit was made publicly available in Exploit-DB for the vulnerability.
Assessment Date	The date that a scan was first initiated that included a plugin to assess the vulnerability.
Time to Assess (TtA)	The time in days between when a vulnerability was publicly disclosed and when a plugin for the vulnerability was included in a vulnerability assessment scan. The plugin release date is the earliest time that a specific vulnerability could have been detected.
Time to Exploit (TtE)	The time in days between when a vulnerability was publicly disclosed and when an exploit for the vulnerability was published.
Affected Asset	The time in days between when a vulnerability was publicly disclosed and when an exploit for the vulnerability was published.
CVE	Common Vulnerabilities and Exposure – a common identifier for publicly known vulnerabilities. CVE and vulnerability are used in this document interchangeably.
CPE	Common Platform Enumeration
CVSS	Common Vulnerability Scoring System. We refer to CVSS Version 2 in this paper.

Table 6. Definition of Key Terms

VIII. ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 24,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver Tenable.io®, the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include 53 percent of the Fortune 500, 29 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

05/03/18 V01

Copyright 2018 Tenable, Inc. All rights reserved. Tenable, the Tenable logo, Tenable.io, and The Cyber Exposure Company are registered trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.