



ANSWERS TO THE MOST POPULAR PREDICTIVE PRIORITIZATION QUESTIONS



Cyber Risk Creates Real Business Risk

Patching all the vulnerabilities present in an organization is difficult because:

- Businesses lack the visibility they need into and across all their technology assets
- Some assets have multiple associated vulnerabilities, so the total number of vulnerabilities is too numerous to manage
- There are too few cybersecurity and IT resources available to identify and patch all vulnerabilities

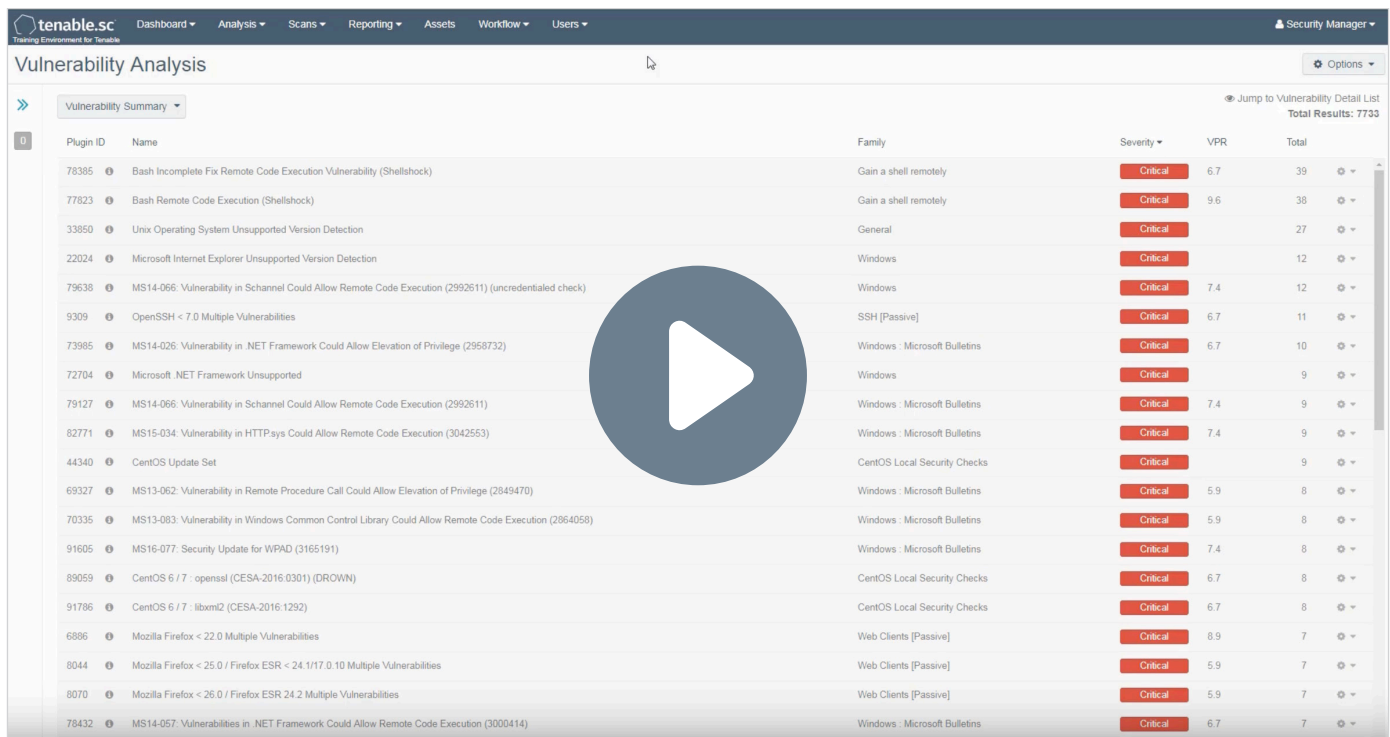
The inability to patch all vulnerabilities creates exploit opportunities. According to a study by the Ponemon Institute, 91% of organizations have experienced at least one damaging cyberattack over the past two years. 60% have had two or more cyberattacks¹.

Q. What is Predictive Prioritization?

A. Predictive Prioritization is the process of re-prioritizing vulnerabilities based on the probability they will be leveraged in an attack.

Q. What is the difference between Predictive Prioritization and a Vulnerability Priority Rating (VPR)?

A. The output of the Predictive Prioritization process is the Vulnerability Priority Rating (VPR), which indicates the remediation priority for an individual vulnerability. VPR operates on a scale of zero to 10, with 10 being the greatest severity. Watch [the video](#) to learn more about VPR.



Plugin ID	Name	Family	Severity	VPR	Total
78385	Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)	Gain a shell remotely	Critical	6.7	39
77823	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	Critical	9.6	38
33850	Unix Operating System Unsupported Version Detection	General	Critical	27	27
22024	Microsoft Internet Explorer Unsupported Version Detection	Windows	Critical	12	12
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Windows	Critical	7.4	12
9309	OpenSSH < 7.0 Multiple Vulnerabilities	SSH [Passive]	Critical	6.7	11
73985	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Windows: Microsoft Bulletins	Critical	6.7	10
72704	Microsoft .NET Framework Unsupported	Windows	Critical	9	9
79127	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)	Windows: Microsoft Bulletins	Critical	7.4	9
82771	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Windows: Microsoft Bulletins	Critical	7.4	9
44340	CentOS Update Set	CentOS Local Security Checks	Critical	9	9
69327	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Windows: Microsoft Bulletins	Critical	5.9	8
70335	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Windows: Microsoft Bulletins	Critical	5.9	8
91605	MS16-077: Security Update for WPAD (3165191)	Windows: Microsoft Bulletins	Critical	7.4	8
89059	CentOS 6 / 7 : openssl (CESA-2016-0301) (DROWN)	CentOS Local Security Checks	Critical	6.7	8
91786	CentOS 6 / 7 : libxml2 (CESA-2016-1292)	CentOS Local Security Checks	Critical	6.7	8
6886	Mozilla Firefox < 22.0 Multiple Vulnerabilities	Web Clients [Passive]	Critical	8.9	7
8044	Mozilla Firefox < 25.0 / Firefox ESR < 24.1/17.0.10 Multiple Vulnerabilities	Web Clients [Passive]	Critical	5.9	7
8070	Mozilla Firefox < 26.0 / Firefox ESR 24.2 Multiple Vulnerabilities	Web Clients [Passive]	Critical	5.9	7
78432	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Windows: Microsoft Bulletins	Critical	6.7	7

Click image to launch video

1. *Measuring & Managing the Cyber Risks to Business Operations*, Ponemon Institute, December 2018

Q. Why do I need a VPR score? Doesn't CVSS already prioritize vulnerabilities?

A. CVSS does a good job capturing the scope and impact of vulnerabilities. It offers a sound explanation of what could happen if a given vulnerability is exploited. CVSS also provides a foundation to gauge the likelihood of a vulnerability being exploited. However, its current application fails to deliver the granularity needed to prioritize effectively. In fact, approximately 60% of all CVEs are rated High or Critical by CVSS.

Predictive Prioritization remains true to the CVSS framework (see figure below), but enhances it by replacing the CVSS exploitability and exploit code maturity components with a threat score produced by machine learning – powered by a diverse set of data sources. This means organizations can make remediation decisions based on the vulnerabilities that:

- Are likely to be exploited
- If exploited, will have a major impact

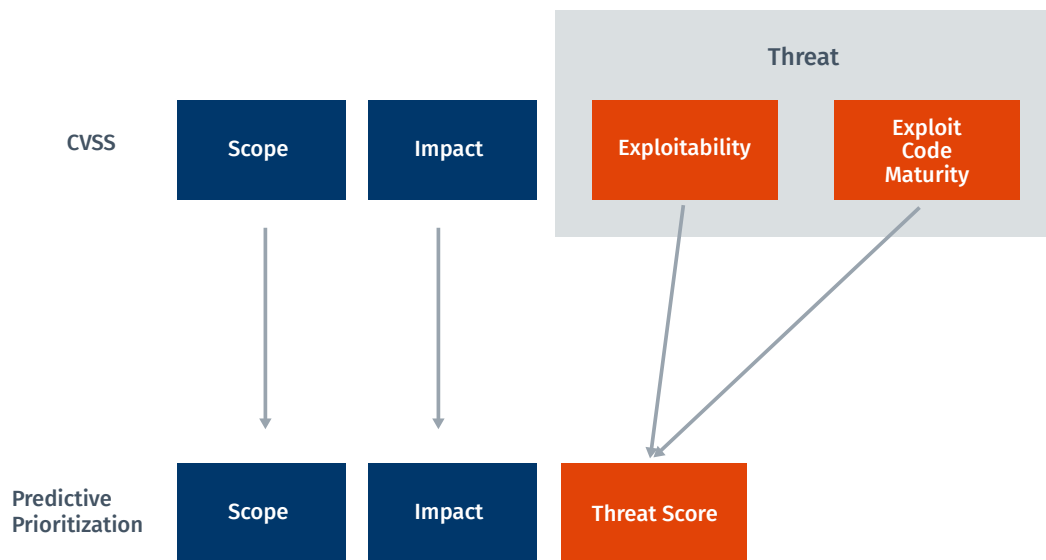


Figure 1. CVSS to Predictive Prioritization Framework

Q. Do VPR scores replace CVSS scores?

A. No. We recommend supplementing your existing processes for prioritization (e.g., CVSS) with VPR.

Q. How do VPR severity bands compare to CVSS severity bands?

A. The same cutoffs are used in CVSS and VPR to create bands. However, the distributions are very different as a result of the prioritization process (see figure below).

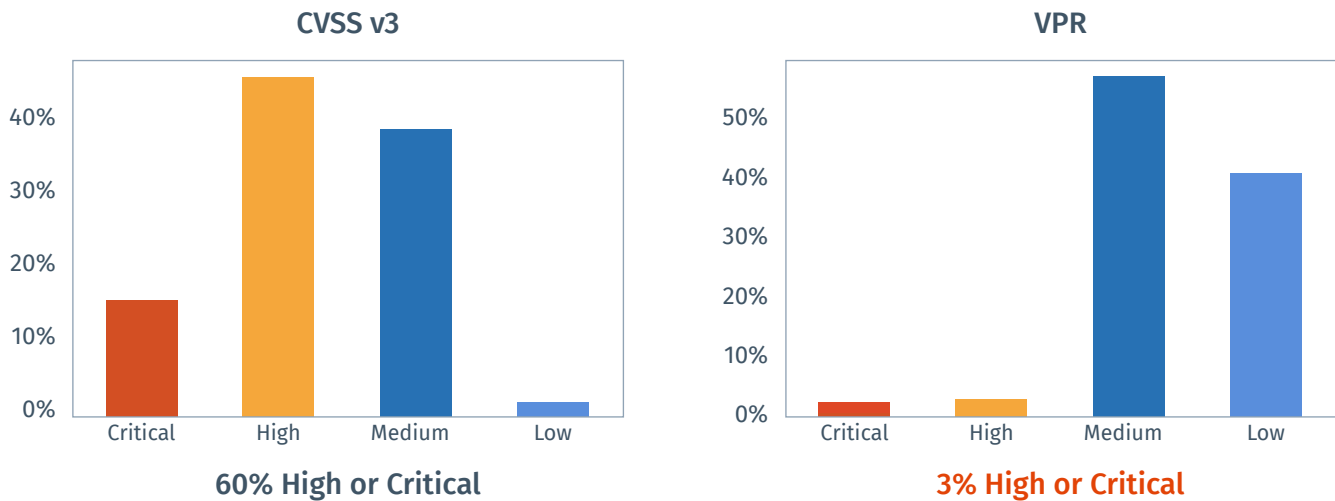


Figure 2. CVSS vs VPR Comparison

Q. Which vulnerabilities get a VPR?

A. Currently, Predictive Prioritization produces a VPR for all vulnerabilities that have a CVE published in the U.S. National Vulnerability Database (NVD). We intend to expand the scope of vulnerabilities scored by Predictive Prioritization in the future.

Q. Can the VPR (score) change?

A. Yes, Predictive Prioritization recalculates VPRs for every CVE every day. They may or may not change, depending on the threat landscape. [Read the technical whitepaper for more information.](#)

Q. Does Predictive Prioritization generate a VPR for CVEs that do not have a CVSS score?

A. Yes. If a CVE has no published CVSS metrics/scores, Predictive Prioritization will generate a VPR using available information (e.g., the vulnerability’s description), which we feed into a model that predicts the scores based on terms that appear in the raw text.

For example, if the vulnerability’s description contains the terms “Adobe” and “arbitrary code execution,” then the model might predict high CVSS scores due to past activity on vulnerabilities with similar characteristics. When the actual CVSS scores become available, they replace our predicted values. This is advantageous, as it typically takes 45 days for NVD to publish CVSS scores following the vulnerability’s publication.

Q. Help me understand VPR scores. What does a Critical (>9) VPR actually mean?

And, what does a Low VPR mean?

- A.** Broadly speaking, a Critical VPR means the vulnerability in question has a high probability of being exploited and/or, if successfully exploited, its impact would be significant.

On the flip side, Predictive Prioritization assigns a Low VPR to vulnerabilities that have a lower probability of exploitation and/or the impact, if successfully exploited, is low. However, please keep in mind we can never say with 100% certainty that a vulnerability will not be exploited.

Q. Tenable says Predictive Prioritization will help me focus on the 3% that matter most.

What does that 3% mean?

- A.** This 3% corresponds to the vulnerabilities with a High or Critical VPR and gives you an idea of which vulnerabilities to prioritize for remediation. We recommend you start fixing vulnerabilities with Critical and High VPRs and work your way down the list. In no way are we suggesting that you should ignore the other 97% of vulnerabilities.

Q. How is VPR different from the CVSS temporal score?

- A.** The main difference between the two is that VPR predicts the future while CVSS only looks at the past. VPR not only considers the availability and functionality of exploit code, but it also predicts the likelihood of exploitation in the short-term future. VPR is also more granular in how it accommodates exploitation.

Q. “Predictive” sounds interesting, but why does it actually matter?

- A.** Instead of just looking at historical data to score vulnerabilities, using historical data and a predictive machine learning-based algorithm helps us anticipate – and plan for – what’s likely to happen (rather than what’s already happened). When managing risk, it’s important to know if something has happened in the past, but it’s much more important to know what’s likely to happen in the future.

Q. Is there a difference between exploitable and being exploited?

- A.** Yes. Exploitable simply means there is an exploit available and could be as basic as an unreliable proof of concept posted to a public archive. But, an exploited vulnerability is serious – it means an exploit successfully breached a vulnerability.

Q. What if a vulnerability has already been exploited?

- A.** While a vulnerability may have been exploited in the past, the likelihood of being actively exploited (i.e., used in cyberattacks) in the future can change over time.

Q. What if a vulnerability has already been exploited?

- A.** While a vulnerability may have been exploited in the past, the likelihood of being actively exploited (i.e., used in cyberattacks) in the future can change over time.

Q. Do you analyze the full history of every vulnerability?

A. We look at all available information since the vulnerability's publication.

Q. What are the inputs into the machine learning model for the threat score?

A. Predictive Prioritization currently uses more than 150 distinct features as inputs into the machine learning model to produce the threat score. A feature (or input) is an attribute of a CVE that allows us to describe or understand it more clearly. Here are a few examples:

- The age of the vulnerability
- Exploit kit availability
- Chatter on the dark web

Broadly speaking, we tend to group features into these categories:

- Past threat patterns (e.g., evidence of exploitation in the past - how recent? how frequent?)
- Past threat sources (e.g., specific sources showing evidence of exploitation)
- Vulnerability metrics (CVSS metrics such as access vector, attack complexity, base score, etc.)
- Vulnerability metadata (age of vulnerability, CVE, vendor/software impacted by the vulnerability, etc.)
- Exploit availability using threat intelligence data (is the vulnerability in Exploit Database? Metasploit?)

Today, that data comes from seven types of sources:

- Information security websites
- Blogs
- Vulnerability disclosures
- Social media
- Forums
- Dark web
- Vulnerability landscape

Q. Where can I find more information about Predictive Prioritization?

A. Please check out the Predictive Prioritization whitepaper, [How to Focus on the Vulnerabilities That Matter Most](#).



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com



08/22/19 V03

COPYRIGHT 2019 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.