Enhancements to Tenable's Vulnerability Priority Rating (VPR)

Quick Reference Guide

Last Revised: July 21, 2025

Table of Contents

Enhancements to Tenable's Vulnerability Priority Rating (VPR)

Tenable released and patented the original version of Vulnerability Priority Rating (VPR) in 2019 to empower security teams to more effectively prioritize vulnerabilities for remediation efforts. Now, in 2025, we're releasing enhancements to VPR, making it twice as efficient as the original version at identifying CVEs that are currently being exploited in the wild or are likely to be exploited in the near term. This FAQ answers common questions about what's changed, how it benefits your risk management strategy, and what to expect moving forward so you can focus faster on what matters most.

Understanding Vulnerability Priority Rating (VPR)

What is Vulnerability Priority Rating (VPR)?

Vulnerability Priority Rating, or VPR, is Tenable's proprietary dynamic risk score that prioritizes vulnerabilities based on threat context and real-world exploitability, helping organizations improve their remediation efficiency and effectiveness.

What makes the enhanced version of VPR more effective than the original VPR?

The latest version of VPR features improved machine learning models, expanded data sources, better context-aware scoring, and refined severity bands to reduce noise, improve accuracy, and drive more confident decision-making:

- **Even More Focused Prioritization** - While static CVSS scores flag 60% of CVEs as High or Critical, original VPR narrowed focus to 3%. Now, enhancements to VPR push efficiency further, leveraging more real-time data to focus teams on just 1.6% of vulnerabilities that truly matter (source).
- **Data Sources** - In addition to data inputs already used for VPR, such as the National Vulnerability Database (NVD), CVSS, exploit databases, and threat intelligence partners, the enhanced version of VPR uses data supplied by the Tenable Research Special Operations team, Tenable Vulnerability Intelligence, cybersecurity web articles and AI news features, CISA, Github, and Mastodon. These new data sources provide greater visibility into which

vulnerabilities are actively exploited in the wild.

- **AI integration** - Generative AI is used to process curated web articles at scale and tag CVEs as targeted by ransomware, exploited in the wild or zero day, among others. This data is used by the new model to predict near-term likelihood of exploitation. Generative AI is also used to provide contextual metadata on CVEs (see below).
- **Score Drivers** - The enhanced version of VPR provides more detailed information on the drivers of each rating. This extra information facilitates greater explainability for the end user.
- **Contextual Metadata** - In addition to information that actually feeds into VPR, generative AI is utilized to provide contextual metadata on the CVE. This includes a threat summary for the CVE that describes the vulnerability and includes pertinent information, such as if it has been targeted by known threat actors in the past. A remediation summary details steps that should be taken to remediate the vulnerability. Lists of targeted regions and industries are also provided. This data is based on curated web articles related to each CVE.
- **Threat Score Influence** - The enhanced version of VPR places equal weighting on the “threat score” (derived from the likelihood of exploitation) and the “impact score” (from CVSS). This is a minor adjustment to the original VPR which places greater weight on the impact score.

How VPR Works

How is the VPR score calculated?

VPR uses a machine learning model that analyzes multiple dynamic factors, including threat actor activity, exploit code maturity, and vulnerability age to generate a predicted likelihood of exploitation. This is combined with the CVSS impact score to arrive at the final VPR.. For example, a low score (0.1-3.9) suggests there is little to no known exploitation. However, a high score (9.0-10.0) indicates that weaponized exploits are observed, with active campaigns targeting the vulnerability.

What data sources are used in the enhanced version of VPR?

The model leverages threat intelligence feeds, public and private exploit databases, open-source data, and proprietary research. To be more specific, data sources include NVD, CVSS, Tenable Vulnerability Intelligence, Tenable Research Special Operations (RSO), web articles, AI news features, AI domain classification, Mastodon, CISA, and Github.

Which vulnerabilities receive a VPR score?

All vulnerabilities with a valid CVE ID (including those not yet published to the NVD) are assigned a VPR score.

How often do VPR scores update?

VPR scores are updated daily to reflect the latest threat intelligence and real-world changes in exploitability.

How should security teams interpret a high vs. low VPR score?

A high VPR score (e.g., 7.0–10.0) indicates urgent action is needed due to high risk of exploitation. Low scores suggest limited or no current threat activity and may be deprioritized.

How do the enhancements to VPR help reduce false positives and alert fatigue?

The enhancements to VPR refine the scoring algorithm to better distinguish high-priority vulnerabilities from low-risk ones, decreasing unnecessary alerts and streamlining remediation workflows. CVSS flags 60% of CVEs as High or Critical, which is a massive number and makes it impossible to prioritize what to fix first effectively. Our original VPR narrowed the focus from 60% of CVEs flagged as High or Critical by CVSS to just 3%, significantly helping teams focus their remediation efforts. With the enhancements to VPR, we're now pushing efficiency even further, focusing teams on just 1.6% of vulnerabilities that represent actual risk to the business. Read our technical white paper for more details.

VPR vs. Other Risk Scoring Methods

How does VPR differ from CVSS and EPSS?

CVSS measures inherent technical severity. EPSS estimates the likelihood of exploitation. VPR combines threat intelligence and exploit prediction using machine learning with business impact to offer more operational, real-time prioritization. Read our technical white paper for more details.

Do VPR scores replace CVSS or EPSS?

No. VPR complements CVSS and EPSS by incorporating real-world threat data and asset context, providing a more comprehensive and actionable view of risk.

How does VPR work alongside CVSS and EPSS?

CVSS is used to understand technical severity, EPSS is used for statistical exploit likelihood, and VPR is for operational prioritization based on real-world threat likelihood and business impact.

What’s the difference between VPR severity bands and CVSS severity bands?

VPR severity bands are tuned to reflect real-world risk, not just technical attributes (they help reduce alert fatigue by focusing attention on genuinely high-risk issues).

Cross-Product Availability and Transition Plan

Will Tenable deprecate the original VPR in Tenable Vulnerability Management? If so, when?

Both versions will coexist over the next few months in Tenable Vulnerability Management, giving customers time to smoothly migrate. Deprecation timing of the original VPR in Tenable Vulnerability Management is targeted for later in 2025. Details will be communicated in advance.

In which Tenable products will the enhanced VPR be made available ?

The enhanced version, referred to in product as ‘VPR (Beta)’, will be generally available in Tenable Vulnerability Management on July 22, 2025. It will be made available in Tenable One later in July, with a target date of July 29, 2025. It will be made available in Tenable.sc later in 2025.

How will existing customers transition from original VPR to the enhanced version?

Tenable provides dual visibility and in-product guidance to help users compare VPR versions, adjust policies, and adapt workflows gradually.

Will customers need to adjust their workflows when using the enhanced VPR?

Some adjustments may be required depending on how VPR is currently integrated into prioritization workflows. Tenable offers documentation and support to ease the transition.

Can I see both version scores in my environment?

Yes. Tenable intends to support both versions (distinguished in product as 'VPR' and 'VPR (Beta)') in parallel over the next few months. Both scores are visible in Vulnerability Intelligence and the Explore view in Tenable Vulnerability Management. Deprecation timing of the original VPR is targeted for later in 2025. Details will be communicated in advance.

How does the enhanced VPR (referred to in product as 'VPR (Beta)') affect my current Asset Exposure Score (AES) and Cyber Exposure Score (CES)?

The current AES and CES scores are not affected by VPR (Beta), as they currently rely on the original VPR version as an input. Any future impacts will be communicated in advance.

When will the enhanced VPR impact other Tenable scores?

The enhanced VPR will be made available on July 29, 2025 in Tenable One as a new property in Weaknesses and Findings pages. We'll provide an update on the timeline for its integration with other Tenable scores as soon as it's available.

Customer Benefits and Implementation

How should I use VPR scores in my patching and risk management strategy?

Prioritize remediation for vulnerabilities with high VPR scores, especially on critical assets, to reduce risk exposure and improve security posture.

Can I customize prioritization rules based on VPR scores?

Yes, Tenable enables users to tailor risk scoring policies, filters, and remediation workflows using VPR thresholds and asset criticality.

Does VPR integrate with ticketing systems and automation tools?

Yes. Both VPR scores (legacy and enhanced) are available via API and supported integrations, enabling automated ticket creation, patching, and risk reporting within tools like ServiceNow, JIRA, and SOAR platforms. The API field name for enhanced VPR is vpr_v2.

Is there a difference between exploitable and being exploited?

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.

What if a vulnerability has already been exploited?

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.

Do you analyze the full history of every vulnerability?

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