
SOLUTION BRIEF

VSCORE PRIORITIZATION

Determine Which Vulnerabilities Should Be Actioned First



VSCORE Prioritization

Vulnerabilities and risk are an everyday reality for the security teams that manage them. The challenge for those assigned with that task is not to become overwhelmed by the growing number or magnitude. Effective risk management requires teams to identify what is going on within the network and to focus on what is most important – those with the most criticality or impact. Only then can remediation plans be put in place to reduce the risk to the organization.

Prioritization in a world of thousands of vulnerabilities identified each year is a necessity even for the most advanced security team. In 2021, the average number of cyberattacks and data breaches increased over 15% from the previous year.

To help us, we need to be able to maintain full visibility into our assets and their associated attack vectors as well as ingest vulnerability intelligence to reduce the time that networks remain vulnerable to attacks. Without this, it is impossible to plan vulnerability remediation.

And while some teams do this manually, it is difficult to scale. Building context around a vulnerability should be integrated into vulnerability management solutions so that it is a seamless part of the process and is automated.

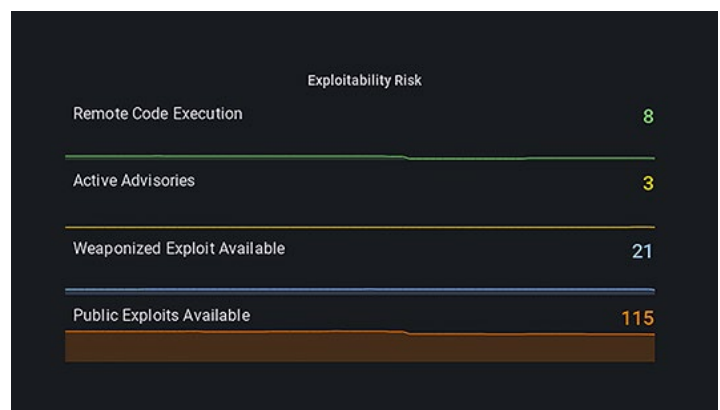


Figure 1. Exploitability Risk Factors

Solution Overview

VULNERA's VSCORE prioritization feature helps teams automatically classify and prioritize threats found within the environment. Vulnerability and risk metrics regarding assets and services connecting to the network (internal, external, and cloud) is collected, aggregated, and compared across the organization in a manner that is accessible and understandable.

The VSCORE allows teams to flag those threats which are most critical to the organization so they may be prioritized for remediation. The ranking provides a visual tool for communicating with stakeholders and provides insight into where resources are needed to manage and mitigate high risk/critical threats. As a result, the security team can ultimately invest limited resources on what demands the most attention and maximize risk reduction.



Figure 2. Remediation Action Required



Figure 3. New Issues by Day and Severity

How It Works

While the Common Vulnerability Scoring System (CVSS) attempts to provide a numerical representation of the severity of vulnerabilities, it does not reflect the risk that a vulnerability poses to an organization nor the likelihood of exploitation. To correctly prioritize vulnerabilities, security teams need to consider multiple sources of threat intelligence.

VULNERA solutions help security teams continuously identify which assets exist within the target environment, analyze the probability of a risk event occurring and the potential impact to the organization, and assign it a VSCORE (risk) score.

VSCOREs incorporate CVSS scores and traditional severity ratings, but also include additional vulnerability criteria including:

- Active exploits available on the internet or in exploit packs

- Are remotely exploitable
- Often result in arbitrary code execution
- Being used in known exploit campaigns
- Have active advisories from vendors and regulating bodies

This allows teams to sort the risks by criticality – identifying those that need the immediate attention of the team. It also serves as an existing scale to evaluate new risks so that they can be quickly assessed and prioritized amongst ongoing activities for mitigation.

The result is speeding the remediation process. These results can also be used as part of the communications plan so all stakeholders have the same view of the level of risk across the organization.

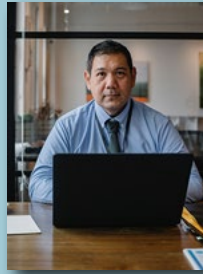
Focus on the Issues that Matter Most

No matter your role on the team, VSCORE prioritization helps satisfy the needs of executives, technology and security teams, and operations and project management teams.



For IT & Security Teams

- Dashboards provide context into risk ratings and a prioritized roadmap for remediation
- Reduces organization's risk profile by addressing the most critical issues first
- Moves beyond a single risk rating



For CISOs

- Contextualized prioritization lessens alert fatigue
- Actionable remediation for threats that pose the most risk
- Reduces stress and shortens the remediation cycle



For Risk & Compliance Teams

- Helps you better understand how pervasive risk is within the organization
- Defined scoring methodology helps defend initiatives and resources needed for your compliance committee
- Identifies the severity and potential impact on the organization

About VULNERA

Security assessments should empower companies to achieve compliance while also improving the security of the organization. The industry is riddled with variances in quality, fragmented offerings, logistical constraints, and resource limitations. That's why VULNERA has built vulnerability management solutions that help organizations with the heavy-lifting so stakeholders can focus on what matters – remediating security issues.

CONTACT

To learn more about how VULNERA helps with classifying and prioritizing risk as well as other security challenges, please visit www.vulnera.com or call +1 626.515. 5523 for a discussion with a vulnerability expert.