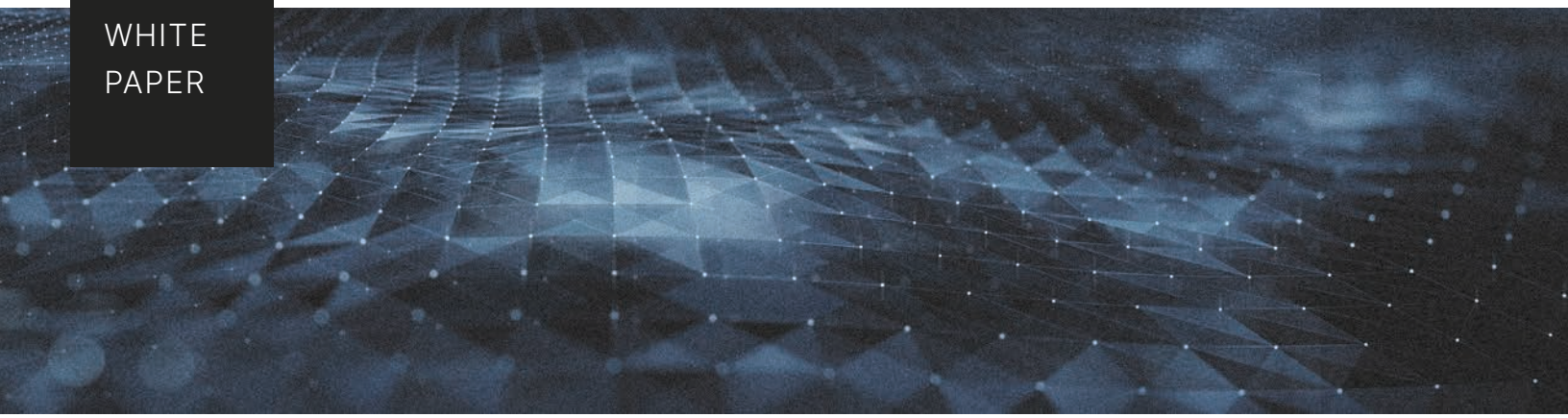
Recorded Future®

WHITE PAPER



Patch What Matters with Risk-Based Vulnerability Management

Today's Digital World Demands Modern Vulnerability Management

Digital transformation initiatives have become a common way for organizations to not only increase business agility, but also to adapt quickly to market changes, environmental forces, and business priorities. Responses to COVID-19, for example, have massively accelerated the adoption of digital technologies by several years.

As organizations transform their enterprises and move to a remote-work model in response to COVID-19, cybersecurity professionals are facing a sudden expansion of their attack surface. In addition to the risk presented by ever-increasing numbers and types of devices and technologies, such as cloud-based applications, software-defined networks, and operational technology, personal devices) continue to alter and increase the attack surface. In a recent survey, 67% of IT professionals reported that remote workers' use of their own devices to access business applications and IT infrastructure decreased their firms' security posture. Further, smart phones, laptops, and mobile devices are the most vulnerable endpoints or entry points to organizations' networks and enterprise systems.[1]

As the attack surface increases, so do the number of vulnerabilities your organization is exposed to, which threat actors are quick to exploit. Vulnerability management teams need to be constantly vigilant and ready to act. However, with more potential points of entry, it's all but impossible to catch all vulnerabilities, let alone prioritize and remediate them in a timely manner. There's no disputing that unpatched vulnerabilities make systems easy prey. Any yet, failure to patch remains a major problem. Industry research, for example, reveals that 60% of breaches were linked to a vulnerability where a patch was available but not applied, up from 57% the prior year.[2] Further, an analysis of 2,013 data breaches shows that more than half (52%) involved some form of hacking. Of the most prominent hacking variety and vector combinations, 'vulnerability exploitation' made the top three.[3]

Legacy Vulnerability Management Can't Keep Pace

Most organizations have zero–or very limited–visibility into vulnerabilities that have not yet been published in the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD). To make matters worse, there is a long delay between vulnerability discovery and CVE (Common Vulnerabilities and Exposures) publication. Recent industry analysis reveals that 80% of public exploits are published before the CVEs are published and that, on average, an exploit is published 23 days before the CVE is published.

The delay between a vulnerability's first occurrence and its initial publication in the NVD is problematic because it makes it difficult for vulnerability management teams to understand which areas of their environment are at risk. Further, they often struggle to keep track of which vulnerabilities have and haven't been patched–leaving dangerous openings for attackers to strike. Industry research backs this up, reporting that the majority (75%) of IT security professionals can't easily track whether vulnerabilities are being patched in a timely manner.[4]

[1] Ponemon Institute LLC, Cybersecurity in the Remote Work Era: A Global Risk Report, October 2020.

[2] Ponemon Institute, LLC, Costs and Consequences of Gaps in Vulnerability Response, April 2018.

[3] Verizon Enterprise Solutions, 2020 Data Breach Investigations Report, May 2019.

[4] Ponemon Institute, LLC, Costs and Consequences of Gaps in Vulnerability Response, April 2018.

Increasing Vulnerability Velocity and Severity

Adding to the challenge, vulnerability severity appears to be increasing. Due to changes made in the industry standard Common Vulnerability Scoring System (CVSS), the majority of vulnerabilities are now categorized as high or critical. Of the 18,000 vulnerabilities identified in 2020, for example, nearly 60% fell into these two categories of severity.

Beyond increasing threat severity, threat actors have gotten faster at exploiting vulnerabilities, leaving IT security teams facing a ticking clock when it comes to remediation. Today, it takes about 15 days for an exploit to appear in the wild once a vulnerability is identified. This means that security teams have only about two weeks to patch or remediate a system against a new vulnerability. Unfortunately, IT security professionals continue to be challenged in this area, with 72% reporting difficulty in prioritizing what needs to be patched, up from 65% the prior year.[5]

With new vulnerabilities being discovered in increasing velocity and volume, scanning tools are returning hundreds, if not thousands–or tens of thousands–of vulnerabilities. It goes without saying that the prospect of quickly remediating every vulnerability identified by a scan is unfeasible. Overwhelmed and already stretched too thin to fix each one, most vulnerability management teams simply prioritize patching based on the CVSS severity levels.

Due to changes made in the industry standard Common Vulnerability Scoring System (CVSS), the majority of vulnerabilities are now categorized as high or critical.

Of the 18,000 vulnerabilities identified in 2020, for example, nearly 60% fell into these two categories of severity.

Why Defenders Need to Look Beyond CVSS

Adopted in 2005, CVSS is used by NIST to rate security flaws in terms of risk and severity. A vulnerability is given a Base Score ranging from zero to 10 that gives an idea of how easily the vulnerability can be exploited and how much damage an exploit targeting that vulnerability could inflict. As an exception rather than a rule, some vulnerabilities are also given a Temporal Score that indicates:

- How aware people are of the vulnerability
- Remedial steps being taken
- Whether threat actors are targeting the vulnerability

Lastly, organizations can modify the Base Score with an Environment Score, which provides a customized metric specific to a business environment. However, many organizations lack the bandwidth to do so.

[5] Ponemon Institute, LLC, Costs and Consequences of Gaps in Vulnerability Response, April 2018.

CVSS is Not Enough

Leveraging CVSS scores to prioritize vulnerabilities makes sense on the surface, but there are serious issues with the rating scheme as the CVSS was never meant to be used on its own for prioritization. To begin with, the CVSS score blurs the distinction between practical and theoretical risk. Relying exclusively on the CVSS score leads to more resources being spent on 'critical' vulnerabilities–and less ability to effectively prioritize the highest risk vulnerabilities. Second, it's important to keep in mind that only 5.5% of all vulnerabilities are ever actually exploited. Without contextual data, IT staff are wasting valuable time on vulnerabilities that pose little to no risk.

Because businesses lack the resources to patch or mitigate everything, it is vital to focus on reducing the most risk possible. The key to vulnerability management is thus the ability to assess the level of risk that vulnerabilities pose to the business. To provide threat-driven, risk-based vulnerability management, IT security teams should factor in the following when prioritizing remediation efforts:

- Asset exposure to threats
- Asset value
- Vulnerability severity

The better the assessment, the better able you'll be able to prioritize the effort to remediate individual vulnerabilities that score above the business risk appetite.

The key to vulnerability management is thus the ability to assess the level of risk that vulnerabilities pose to the business.

CVSS System Shortcomings

Recognizing that remediating all vulnerabilities is neither feasible nor cost-effective, it's clear that CVSS scores are simply 'not enough' to evaluate threats properly as technical severity does not equal risk to your business. Shortcomings of the CVSS scoring system include:

- Exploitability versus exploitation
- Lack of timeliness/delay in reporting
- Static base scores
- Assumption of widespread exploitation
- Failure to consider relationships between vulnerabilities
- Lack of critical business context

Exploitability Versus Exploitation: Information in vulnerability databases is almost entirely focused on technical exploitability–a judgement of how likely it is that exploiting a particular vulnerability will result in greater or lesser damage to systems and networks. But technical exploitability and active exploitation are not the same thing. Unless a Base Score is modified by a Temporal or Environmental Score, it really only tells you how bad the vulnerability is hypothetically – not whether it's actually being exploited in the wild.

IT security teams are continuously faced with the challenge of keeping up with countless patch updates without knowing which vulnerabilities are actually being exploited by threat actors. The missing link is the overlap between the vulnerabilities in the systems being used and the ones that are actively being exploited. This information can help you prioritize resources to make informed, data-driven decisions on remediating systems.

Lack of Timeliness and Delay In Reporting: Vulnerability databases are not updated quickly enough to provide warning of quickly spreading threats. The informal way in which vulnerabilities are disclosed and announced contributes to the delay in recognizing them in vulnerability databases. Typically, a vendor or researcher discloses the vulnerability to the NVD, which assigns a CVE number and begins analysis. In the meantime, the originator publishes more information on their own blog or social media account. Research from Recorded Future reaffirms this, reporting that 75% of disclosed vulnerabilities appear on other online sources (social media, researcher blogs, Dark Web, etc.) before they appear in the NVD.

Static Base Scores: CVSS scores fail to reflect the current threat landscape. The Base Score is typically assigned within two weeks of the vulnerability being discovered and is almost never revisited after the initial assessment–even if circumstances or the threat landscape changes. That means that if a vulnerability was initially assigned a Base Score of 5.0, it will remain at the initial 5.0 – even if several months later it's successfully exploited in the wild and even if it becomes a prolifically exploited vulnerability that causes widespread damage.

Assumption of Widespread Exploitation: Temporal Scores are designed to lower the Base Score by addressing whether threat actors are actively weaponizing the vulnerability and the likelihood of active exploits. If considered at all, the default value of the Exploit Code Maturity metric in the Temporal Score assumes widespread exploitation, which is unrealistic. Since more than 75% of all vulnerabilities with a score of seven or above have never had an exploit published against them, security teams using CVSS to prioritize efforts are wasting the majority of their time chasing after the wrong issues.

Failure to Consider Relationships Between Vulnerabilities: CVSS does not consider relationships between vulnerabilities that allow threat actors to pivot or to escalate privileges. Nor does it consider issues that are not strictly defined as vulnerabilities, such as insecure misconfigurations. These both play a role in evaluating the risk status and prioritizing response.

Lack of Critical Business Context: CVSS scores are subjective. Unless the organization modifies the Base Score with an Environmental Score, it fails to consider critical context around the assets that the vulnerability is exposing. When it comes to using the CVSS score to prioritize remediation efforts, time and time again, vulnerabilities with CVSS scores ranging from 7 to 10 are given top priority, even if the affected assets would only cause minimal impact to the business if compromised. Meanwhile, vulnerabilities with CVSS scores of 5 sit lower on the priority list even though they could expose high-value assets and targeted exploits are actively being weaponized.

Align Vulnerability Management with Business Risk

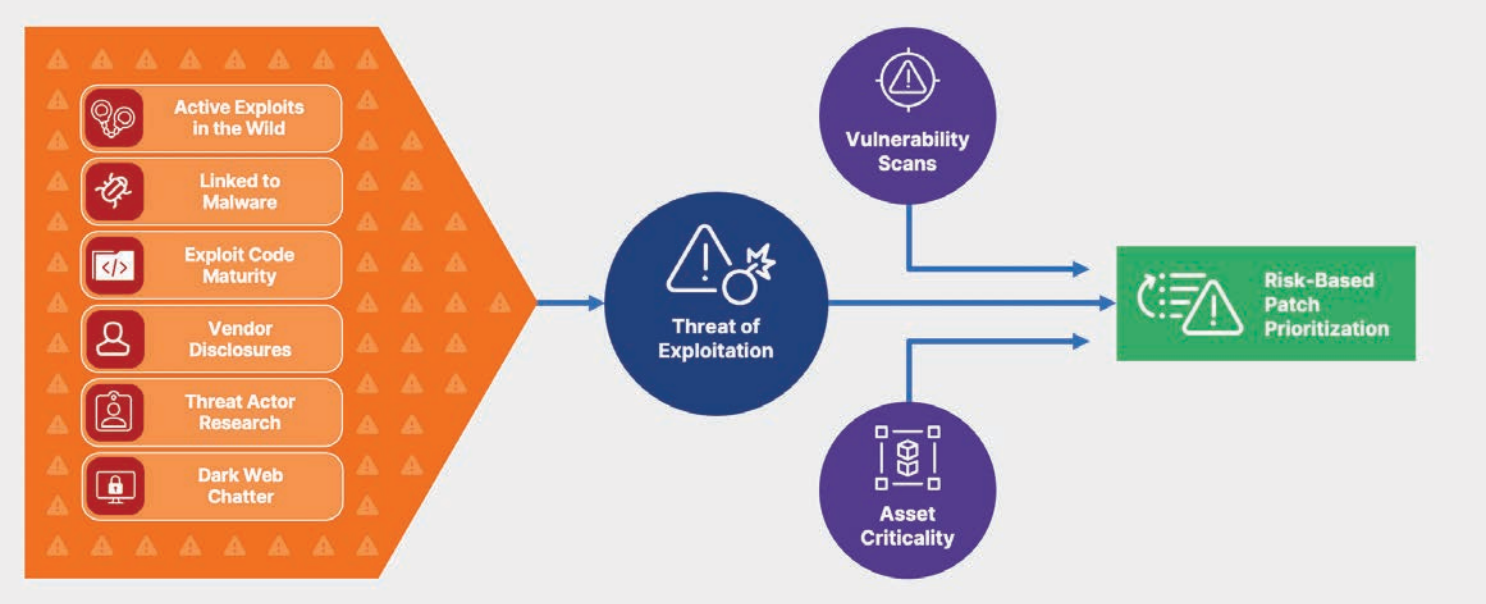
CVSS scores can provide a starting point for evaluating how bad a particular vulnerability is. It's important to keep in mind that CVSS was never meant to measure risk to a certain organization; it was meant to measure the technical severity of the vulnerability. While the familiar 0-10 scoring format has served well in the past, it no longer reflects the way modern networks and applications are built, maintained, and attacked.

Official vulnerability databases, even conventional scanning tools, cannot arm you with the one key metric necessary to prioritize remediation: the overlap between the vulnerabilities in your systems and the ones being actively exploited by threat actors. Because less than 1% of vulnerabilities have been weaponized within the past month–or year–insight into weaponization is essential to adequately prioritize which vulnerabilities to patch.

Prioritize Patching with Risk-Based Vulnerability Intelligence

Prioritizing patching using CVSS alone is insufficient because it doesn't take into account whether a vulnerability is being exploited in the wild. Nor does it understand if the vulnerability is on a business-critical service or system. What's needed is a new system that incorporates risk-focused contextual information specific to your environment to show you where your business is most at risk. That's where risk-based vulnerability intelligence comes into play.

Vulnerability intelligence should not simply provide more information in the form of scores and statistics, but rather a deeper understanding of how and why threat actors are targeting certain vulnerabilities and ignoring others. By combining your company's internal asset criticality and internal vulnerability scanning data with external intelligence from various sources, IT security teams can assess the true risk of a vulnerability to the organization and strike the correct balance between patching vulnerable systems and interrupting business operations.



This diagram shows all of the inputs and data points that lead to risk-based patch prioritization.

Sources of Vulnerability Intelligence

Valuable sources of information for assessing true risk to your business include:

- Information security sites, like vendor blogs, official disclosure sites, and security news sites.
- Technical feeds that deliver data streams of potentially malicious indicators, which add useful context around the activities of malware and exploit kits.
- Code repositories such as GitHub, which yield insights into the development of proof-of-concept code for exploiting vulnerabilities.
- Paste sites such as Pastebin and Ghostbin, that house lists of exploitable vulnerabilities.
- Social media, where link sharing provides jumping off points for uncovering useful intelligence.
- The Dark Web, composed of communities and marketplaces with a barrier to entry, where exploits are developed, shared, and sold.
- Forums with no barrier to entry or requirement to use specific software, where threat actors exchange information on vulnerabilities and exploits.

The Business Benefits of Vulnerability Intelligence

Implementing vulnerability intelligence into company workflows doesn't just help identify zero-days; it radically shifts the way vulnerability management programs operate. By leveraging vulnerability intelligence and moving to a risk-based approach to vulnerability management, organizations can:

- Reduce the most possible risk by prioritizing patching based on threat severity.
- Minimize expensive off-cycle patches.
- Justify patching decisions with transparent evidence.
- Improve team efficiency and simplify workflows.
- Maximize the investment in existing security tools.

Vulnerability intelligence from Recorded Future empowers you to defend your organization by prioritizing the vulnerabilities that represent real risk to your business.

Summary

There's a new vulnerability for every day of the week. Yet, severity ratings don't tell the full story and vulnerability databases can't publish fast enough to enable proactive response. Data from asset scans and external vulnerability databases are only the starting points for generating intelligence that enables you to assess the risk of vulnerabilities. Unless vulnerability intelligence includes data from a wide range and variety of sources, you risk missing emerging vulnerabilities until it's too late. True risk-based vulnerability management goes beyond assessing risk based on CVSS scores. It requires looking at internal risk criticality while monitoring external threat trends and vulnerability weaponization that continuously change the risk landscape.

In deciding what to address first, you must weigh the balance between the likely impact of a vulnerability being exploited against the potential operational impact of remediating. This is most effectively achieved by combining internal data from vulnerability scanning and asset criticality with contextualized external intelligence to reveal whether internal vulnerabilities are actually being exploited. By taking a risk-based approach to vulnerability management, you can address the organization's true business risk and focus on the vulnerabilities and assets that matter most.