IBM Security Services

Remediation management: Prioritize and fix vulnerabilities that pose an imminent threat

Save time and resources with a repeatable and auditable process

Table of contents

Executive summary

It takes only one unpatched vulnerability for criminals to compromise an enterprise. The opportunity to do so is abundant. In 2018, IBM X-Force Red found that 14 percent of an average of 1.7 million vulnerabilities scanned had exploits associated with them. If just one within that 14 percent isn't prioritized and remediated, then the risk of a compromise elevates dramatically.

Prioritization and remediation management are key components of an effective vulnerability management program. Ranking vulnerabilities provides organizations with an actionable understanding of which ones should be remediated first. It enables security leaders to focus their limited resources and time on vulnerabilities that, if exploited, would impact the business the most. When vulnerabilities are prioritized, quick and manageable risk-based remediation should follow. Together, these often-overlooked activities can make a real difference in an operation's efficiency, compliance and most importantly, protection of its infrastructure.

Client needs and challenges

The need to prioritize vulnerabilities — from identification to remediation

It’s common to discount the importance of vulnerability management. Executives may underestimate the sheer number of vulnerabilities in their own organizations. They might not consider extra risks that may stem from mergers and acquisitions with other firms.

These individuals will get some sobering facts, particularly in light of industry compliance mandates, such as the General Data Protection Regulation (GDPR). The GDPR requires organizations to protect the personal data and privacy of European data subjects. Failing to comply with the GDPR can cost an organization up to 20 million euro or 4 percent of global annual turnover, whichever is higher.

Scanning systems, applications and networks is the first step. It’s a critical activity for any organization. Scanning can help detect vulnerabilities that come from several factors—from using third-party vendors to overhauling infrastructure.

65,000

Approximate number of vulnerabilities related to end-of-life applications and systems

Source: IBM X-Force Red Vulnerability Management Services engagements in 2018

After scanning an organization’s data for vulnerabilities, the results can be enormous. For large enterprises, a scan may uncover millions of vulnerabilities. Some scan results are so large that they can’t be exported and opened by conventional programs.

6,000,000 +

Number of vulnerabilities found when running scans on one investment firm

Source: IBM X-Force Red Vulnerability Management Services engagements in 2018

Adding to that dilemma, organizations may lack the personnel and expertise to perform a scan, analyze the results and respond. They manually wade through the vulnerabilities, which may take days or even weeks for more than one person to do. This slow process wastes precious time for all parties involved and can leave important assets exposed for even longer, giving criminals more opportunity to attack.

Data that’s manually curated can also become stale quickly. Creating a spreadsheet to rank vulnerabilities might take three to five full workdays to complete. By the time the spreadsheet is finished, new vulnerabilities will likely arise and could be overlooked.

Another complicating factor is lack of expertise. Oftentimes, company leaders believe that when vulnerabilities are found, they’re easy to patch. As such, staff members who lack patching skills and training might receive the assignments instead of experienced data scientists. These inexperienced workers are often not equipped to fix flaws when they’re found.

Many organizations also have a false-positive problem. They spend time chasing down vulnerabilities that aren’t truly vulnerabilities. The same problem occurs when addressing minimal-risk vulnerabilities. This approach wastes time and resources and could leave other critical vulnerabilities unpatched for even longer.

252,000 +

Number of vulnerabilities found when running scans on one bank

38,000

Approximate number of total vulnerabilities with associated exploits at the same bank. Vulnerabilities with exploits exposing high-value assets should be fixed first.

Source: IBM X-Force Red Vulnerability Management Services engagements in 2018

Given these circumstances, many organizations receive a long list of vulnerabilities that don’t get adequately addressed. To help improve their security posture, organizations should implement a vulnerability management program that focuses on:

- Identifying vulnerabilities
- Prioritizing the most critical vulnerabilities based on weaponization and asset value
- Following a manageable remediation process to fix the vulnerabilities that elevate risk the most

Limitations of current prioritization

Network scanners produce results that reference findings by their Common Vulnerabilities and Exposures (CVE) designation. This reference system provides each publicly known security vulnerability with a standardized name. Sponsored by the National Cyber Security Division of the United States Department of Homeland Security, CVE is a useful method for cataloging and managing known vulnerabilities.

Each CVE finding is annotated using the Common Vulnerability Scoring System (CVSS). This industry-recognized standard is used worldwide to rate the severity and risk of CVE based on a formula. The CVSS generates a numerical criticality score based on many factors, including the following:

- Type of attack
- Level of access required
- Overall complexity

The CVSS scores rank vulnerabilities from zero to 10. A 10 indicates the vulnerability is the most critical.

Given its convenience and industry standing, many managers solely rely on the CVSS to rank and prioritize their vulnerabilities. Although the CVSS can be a helpful metric, users need to understand its limitations for prioritization.

First, the CVSS doesn't inherently support a risk-based approach to vulnerability management. The CVSS allows researchers to report the potential to exploit any flaw found and agree on its score. That initial score doesn't account for which exposed assets are the most important to the business. While the CVSS does offer environmental factors that can be used to adjust the score, X-Force Red hasn't witnessed an environment that uses this metric at scale. Also, when anecdotally using these environmental scores, they don't adjust the resulting value enough to have a significant impact on risk prioritization. Without this data, results using the CVSS treat all assets equally, even though some, if compromised, would create much more impact.

Additionally, the CVSS doesn't consider weaponized vulnerabilities. These vulnerabilities are the ones actively being exploited by attackers. The CVSS doesn't differentiate between weaponized and non-weaponized vulnerabilities, even though weaponized vulnerabilities are being used by criminals in the present moment to compromise organizations. Again, the CVSS environmental scores can help, but X-Force Red has found they're rarely used in this capacity and don't significantly adjust overall risk prioritization.

These two factors—asset value and weaponization—can potentially lead to prioritizing the patching of vulnerabilities with low likelihoods of being exploited, exposing less important assets or both. Conversely, truly critical vulnerabilities might remain unpatched, exposing highly sensitive assets for even longer.

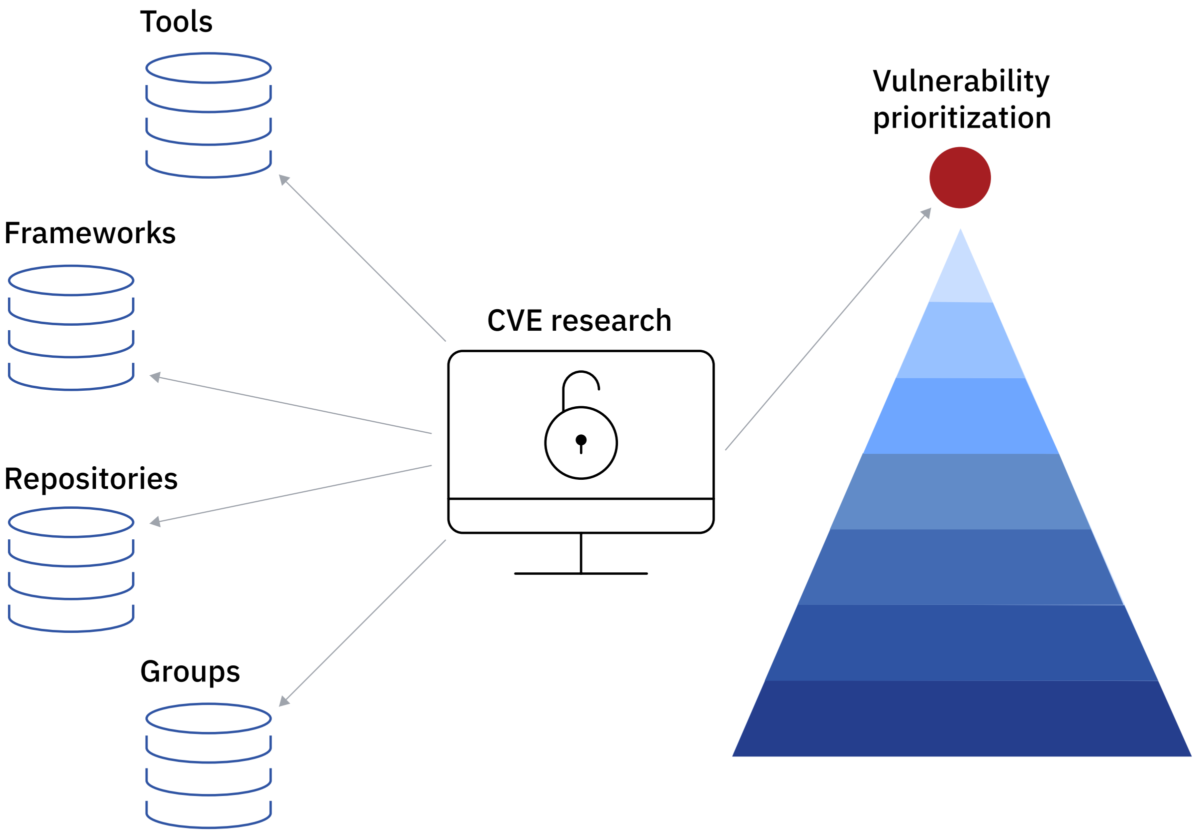

Figure 1. An attacker-minded approach to vulnerability ranking is designed to produce a clear indication of criticality, allowing teams to focus on vulnerabilities that elevate risk the most.

Most commonly targeted vulnerabilities

A more helpful approach will use correlated exploits to rank vulnerabilities being exploited "in the wild." A 2018 Gartner report emphasizes the importance of this approach with the following comments:

- "A vulnerability is only as bad as the threat exploiting it and the impact on the organization."
- "Vulnerability rating schemes that don't take into account what threat actors are leveraging in the wild can cause organizations to address less risky issues first."
- "Implement a risk-based approach that correlates asset value, the severity of vulnerabilities and threat actor activity via the use of threat intelligence and analytics to calculate a realistic risk rating."[1]

The following statistics, gathered by X-Force Red during vulnerability management engagements in 2018, demonstrate the need for prioritizing vulnerabilities based on weaponization and asset value:

1,678,890

Total number of vulnerabilities identified in scan reports in 2018

269,605 (16%)

Total number of vulnerability occurrences that have associated public exploits

2,579

Total number of distinct vulnerabilities found in scan reports. These vulnerabilities are the unique IDs reported by scanners.

590 (23%)

Total number of distinct vulnerability findings that have associated public exploits

A primary takeaway from these numbers is that 16 percent of the vulnerabilities observed have public exploit information associated with them. While that number seems low, if a criminal were to exploit just one of that 16 percent, the damage might be significant. Similarly, roughly one in four findings from scanners can be considered "weapon-ready."

The percentage of weaponized vulnerabilities is low. By correlating and prioritizing the weaponized vulnerabilities exposing an organization's most important assets, remediation should be manageable and effective. This approach places the focus on vulnerabilities that present the most risk.

Vulnerabilities and remediation management

If an outside remediation management provider uses "staff augmentation" of hourly workers, those workers may use scanning tools provided by the client or bought from a vendor. The remediation services provider then interfaces with the ticketing system or spreadsheet clients' scanners use. This process may not be sufficient to produce results because scanners may not be able to find "not yet known" vulnerabilities and aren't designed to protect against hacker mindsets and motivations.

Organizations must begin approaching vulnerability management as a multistep process, not a one-time scanning effort. Based on the sheer number of existing and new vulnerabilities, an effective program will focus the organization's efforts on the most high-risk vulnerabilities in an ongoing fashion.

A main vulnerability remediation challenge is that typically enterprises lack time and resources to dedicate to the process. After prioritizing vulnerabilities based on weaponization and asset value, organizations need to remediate their top vulnerabilities in a concurrent fashion.

Consider this analogy. Imagine a parking lot with spaces for 20 cars, with each vehicle representing a remediation task. Under a concurrent remediation model, remediation tasks arrive and leave all the time, like cars in the lot pulling in and out of their parking spaces. When one car leaves—or when the most critical vulnerability is resolved—the task goes away, and the next most important vulnerability takes its place, like the next car parking in the lot.

By fixing vulnerabilities in small, prioritized batches, the workload is manageable, and the most critical vulnerabilities are remediated first. That process, coupled with the prioritization of vulnerabilities based on weaponization and asset value, offers effective, efficient, risk-based vulnerability management.

IBM solution: IBM X-Force Red Vulnerability Management Services

X-Force Red Vulnerability Management Services is a multistep service delivered by X-Force Red, a team of veteran hackers within IBM Security. This global team identifies, ranks and helps facilitate the remediation of vulnerabilities using an "attacker's mindset." Organizations hire X-Force Red to compromise their businesses by exploiting the same vulnerabilities used by attackers. By understanding how criminals exploit vulnerabilities and which vulnerabilities are being exploited, X-Force Red offers a unique perspective for vulnerability management.

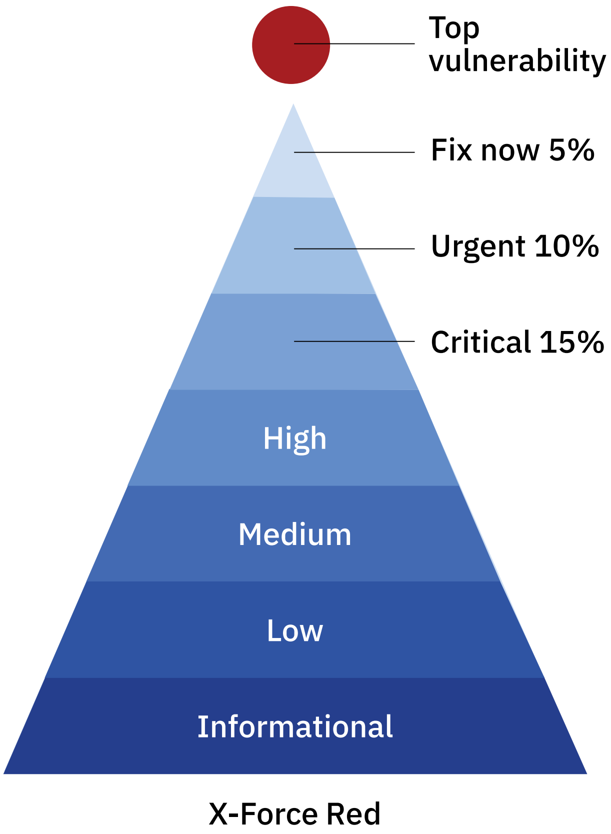

Figure 2. X-Force Red Vulnerability Management Services ranks vulnerabilities based on whether the vulnerabilities are weaponized and the value of the exposed asset. Using a proprietary ranking algorithm, X-Force Red automatically prioritizes vulnerabilities and helps security teams remediate the most critical vulnerabilities first.

As part of X-Force Red Vulnerability Management Services, the team automatically ranks vulnerabilities within minutes, using a proprietary, patent-pending algorithm. The formula includes correlating information from an organization's asset databases, configuration management databases (CMDBs), threat intelligence feeds and more to rank vulnerabilities based on asset value and weaponization.

X-Force Red Vulnerability Management Services also includes data validation. X-Force Red experts manually identify, verify and eliminate false positives so that only truly critical vulnerabilities remain on the priority list. By delivering only legitimate and critical vulnerabilities, X-Force Red can help organizations save time and resources.

When vulnerabilities are validated and ranked based on asset value and weaponization, X-Force Red delivers a prioritized list so that clients know which vulnerabilities to focus on first. Each vulnerability entered includes a title, severity ranking, category, associated threat, proposed solution and remediation schedule. Vulnerabilities with a low CVSS score may sit at the top of the list for remediation if they affect a high-value asset and are being weaponized.

X-Force Red remotely accesses all scanners and their ticketing systems for prioritization and remediation. If no ticket system exists with the scanner, X-Force Red can track the progress using spreadsheets as needed, which allows the program to begin quickly. Either method allows X-Force Red to create a remediation track that follows the lifecycle from discovery to fixing every critical vulnerability found. Additionally, these tools can be run inside client networks when required by privacy standards.

X-Force Red Vulnerability Management Services also includes concurrent remediation. When vulnerabilities are prioritized, X-Force Red provides remediators with manageable lists of the most critical vulnerabilities to fix first. After those vulnerabilities are fixed, X-Force Red sends remediators the next batch.

Concurrent remediation is available in blocks of 20 tasks per each package bought. This approach enables the prioritization and remediation of the most pressing vulnerabilities in a manageable, consistent and efficient fashion. Even with a small remediation team, organizations can fix the most critical vulnerabilities first to help minimize the risk of a compromise.

Conclusion

Given that many organizations have potentially millions of vulnerabilities, many of which expose highly sensitive assets, the need for prioritization and efficient remediation of such flaws is evident. Organizations can achieve that goal by ranking the most critical vulnerabilities based on essential factors, such as asset value and weaponization, and then implementing a concurrent process to fix those vulnerabilities first.

X-Force Red Vulnerability Management Services incorporates attacker-minded expertise and algorithms to help organizations adopt a more efficient and effective vulnerability management program. The result can help save organizations time and resources and, most importantly, minimize the risk of a compromise.

For more information

To learn more about remediation management, please contact your IBM representative or IBM Business Partner, or visit **ibm.com/security.**

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2019

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] Prateek Bhajanka and Craig Lawson. “Implement a Risk-Based Approach to Vulnerability Management.” *Gartner*, August 21, 2018. ibm.com/account/reg/us-en/