CYRISMA

Vulnerability and Patch Management

WHITEPAPER

Vulnerability Management covers the complete cycle of identifying, classifying, analyzing and mitigating security vulnerabilities in an organization's IT environment (computer systems, devices, applications), with the end goal of closing security gaps and reducing cyber risk.

As IT environments have become more complex with a wide range of connected components, extended networks, and dispersed workloads, the concept of "Risk-Based Vulnerability Management" has gained in popularity. Addressing every single vulnerability in complex environments can quickly become overwhelming. As a result, organizational context has become more important when assessing risk, and organizations are increasingly prioritizing and managing vulnerabilities based on a close evaluation of risk to their own specific environments.

Even as new security paradigms emerge, however, the fundamentals of effective vulnerability management remain the same. Systematically implementing the key steps in identifying, assessing and mitigating vulnerabilities is among the most effective ways to reduce cyber risk.

In this whitepaper, we talk about the components of an effective vulnerability and patch management program. The paper is divided into three sections:

- Vulnerability Management
- Patch Management
- Vulnerability Management using CYRISMA

Vulnerability Management

Vulnerability management is one of the foundational security strategies that IT and security teams implement before moving on to controls that are deemed more advanced.

Because cyber threats evolve quickly and new vulnerabilities emerge constantly, the vulnerability management process must be ongoing. By performing vulnerability scans and taking risk mitigation steps regularly, organizations can both keep their critical assets secure and meet regulatory compliance requirements.

Vulnerability Management Lifecycle

The Vulnerability Management Lifecycle is a continual process that enables proactive, structured and controlled cyber risk reduction. It includes identifying vulnerabilities in IT assets; assessing and analyzing the risk posed by these vulnerabilities; and taking steps to mitigate or remediate vulnerabilities.

Identifying Vulnerabilities in IT assets

- **Asset Discovery** - Vulnerability identification presupposes the existence of a regularly updated asset inventory that lists all the IT assets and devices used within the organization or connected to the internal network. The inventory must also include the software applications and operating systems that run on each asset. To ensure that vulnerability scans cover all organizational assets, it is recommended that organizations run asset discovery scans to identify all network-connected assets, and classify assets by criticality.
- **Vulnerability Scanning** – With visibility into all connected assets, IT teams can run vulnerability scans to automatically identify security weaknesses in each of these assets, applications and systems.
- IT environments may include multiple components at different layers that can only be seen and accessed in their entirety using different kinds of scans. To get a complete view of vulnerabilities that are present in their extended IT environments, organizations should have

options for internal, external, authenticated, unauthenticated, agentless, and agent-based scans.

- **Internal Scans** – Internal vulnerability scans identify and analyze vulnerabilities that are present within an organization's network. They analyze how attackers who are already within the network could do greater damage using malicious software and other security holes.
- **External Scans** – External vulnerability scans analyze outward-facing systems and IP addresses and help identify vulnerable network ports or servers that attackers can target from outside the network perimeter.
- **Authenticated Scans** test systems for vulnerabilities (such as broken access controls) that can be seen or exploited by authenticated users. Authenticated scans provide a detailed view of security gaps and system information and can get to the root cause of vulnerabilities.
- **Unauthenticated Scans** find vulnerabilities that can be exploited by threat actors who do not have access to systems. They help identify weaknesses like open ports, vulnerable software, misconfigurations and more.
- **Agent-based scans -** Agent-based scanning involves installing agents (data collectors) on individual host machines or end user devices such as laptops, servers, PCs to collect vulnerability information.
- **Agentless scan -** In agentless scans, vulnerability information can be collected using a single agent to scan multiple network-connected machines as well as IP ranges for the discovery of network assets and unauthenticated vulnerabilities.

- Most organizations use a combination of agentless and agent-based scanning to get the best results. Remote machines that are off-network need their own agents for vulnerability discovery. Machines that are within an organization's network can have agents installed or be scanned via an agent installed on another machine connected to the same network.

Assessing risk and planning mitigation

No organization can patch every single vulnerability that exists in its systems. A successful vulnerability and patch management program depends as much on an organization's ability to prioritize vulnerabilities based on severity and context, as its knowledge of which vulnerabilities exist in the network and patching ability. A thorough risk assessment and prioritization exercise must precede patch deployment.

a. **Vulnerability Assessment and Prioritization** - Organizations must assess risk based on a range of factors that determine how damaging the exploitation of a vulnerability could be (impact), and how likely it is to be exploited (likelihood). IT and security teams today can use a range of tools to get complete context into the root causes of vulnerabilities, their criticality to the organization, how others have been impacted by the same vulnerabilities, and more. A few factors that can be used for assessment and prioritization are:
    a. Vulnerability scores and severity ratings (such as CVSS scores)
    b. Number of assets that are affected by each vulnerability
    c. The presence of mitigating factors or, conversely, factors that increase risk such as other related vulnerabilities
    d. Whether or not the vulnerability is being exploited in the wild
    e. Other threat intel and community knowledge
    f. Organizational or industry context
b. **Planning mitigation or management** – Mitigation planning includes making decisions about what to patch, which high-priority vulnerabilities to patch first and setting a schedule

accordingly, upgrading vulnerable software to prepare it for patching, strengthening configuration settings prior to patching, accepting risk and other mitigation options.

Implementing the mitigation plan

(Patch Management is discussed in greater detail in a later section.)

a. Preparing the IT infrastructure for mitigation-related changes includes:
    a. Determining exactly which assets need patching and preparing both systems and system owners for deployment
    b. Scheduling and coordinating patch implementation and response activities to minimize interference with regular operations
    c. Testing patches before deploying them
b. Response steps may include:
    a. Patch deployment
    b. Updating and upgrading systems
    c. Changing configuration settings to make systems more secure
    d. Other risk mitigation activities
c. Verifying that mitigation steps were executed successfully
    a. Running repeat vulnerability scans to ensure patching was successful
    b. Testing additional security controls that were implemented
    c. Monitoring systems to ensure the risk response is maintained and any drift is avoided

An Overview of CVEs and CVSS Scores

Two acronyms that are commonly used by IT and security practitioners in the context of vulnerability management are CVE and CVSS. Known vulnerabilities are tracked by their CVE IDs, and conversation about their criticality may often begin with what is known as a CVSS score. Here is a brief description of the two terms.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) list is an open catalog of publicly disclosed vulnerabilities and exposures, maintained by the MITRE Corporation. Each individual CVE record (or trackable vulnerability) is added to the list by a CVE Numbering Authority (CNA) - a vendor, researcher, CERT or other organization authorized by the CVE Program to assign IDs to and publish vulnerabilities. A CVE record must include “an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities.”

National Vulnerability Database (NVD) - A related program is the United States National Vulnerability Database (NVD), which is maintained by NIST and is built upon and fully synchronized with the CVE List. NVD provides “enhanced information for each CVE record such as fix information, severity scores, and impact ratings.”

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is an open framework designed to represent the attributes and severity of software vulnerabilities in numerical scores ranging from 0 to 10, 10 being the most critical. It is is owned and maintained by the **Forum of Incident Response and Security Teams (FIRST)** – a nonprofit organization created with the mission of helping CSIRTs across the world.

CVSS scores are used by organizations to prioritize vulnerabilities as they are published.

Patch Management

A “patch” is an update or a code snippet that can be applied to software or operating systems to fix a security vulnerability.

Patch deployment should ideally be proactive rather than reactive. This means that routine patching as part of an ongoing vulnerability management program is preferable to emergency patching performed in response to an incident.

Patch Management is the process of planning for, prioritizing, testing, deploying and verifying patches after vulnerabilities are discovered and analyzed. It is part of the remediation and mitigation stage of vulnerability management. By deploying patches regularly, organizations minimize the risk of security incidents that could be costly in terms of operational, monetary, legal and reputational damage.

Patch Management Stages

Just as Vulnerability Management involves several steps, Patch Management too starts with the preparation stage, followed by the actual distribution and deployment of patches and, finally, verification that the patches were installed successfully.

Preparation

- Preparation includes first prioritizing patches – much of this is done during the vulnerability assessment process – and then scheduling them. Setting a patch schedule requires IT/security teams to coordinate with business units that would be affected while the patch is being deployed.
- Organizations also need to acquire patches and ensure their authenticity during this stage.
- Finally, the patches may be tested to ensure everything runs smoothly during deployment.

Deployment

While the deployment processes for different kinds of patches can vary quite a bit, some common steps include patch distribution, installation, system changes, and the resolution of any issues that arise following deployment.

- Distributing patches to the assets that are affected by vulnerabilities can either be done by the organization (automatically or manually) or by the software vendor (often via the cloud). Patch distribution can be a smooth process if all IT assets have been systematically inventoried.
- Patch installation, again, can be either manual or automatic, and is initiated by a user, administrator, vendor, or tool. Depending on the affected software and the patch being installed, deployment sometimes requires administrative privileges or user participation.
- After the patch is installed, affected machines or operating systems may need to be rebooted or restarted for the patch to take effect. However, this isn’t needed in all cases.
- Finally, if patch installation leads to undesirable side-effects such as new security issues or operational roadblocks, the IT team may need to roll back a patch or look for workarounds to resolve the problem.

Verification and Monitoring

Once the patch is deployed, the organization should rescan the affected assets to ensure that the patch is in place and working as expected, and that the related vulnerability has been adequately addressed. Systems must also be regularly monitored to prevent drift and detect inadvertent modifications that may affect the efficacy of patches.

CYRISMA's Vulnerability and Patch Management capability

The CYRISMA Platform enables holistic cyber risk reduction with a set of powerful tools that cover asset discovery, vulnerability and patch management, sensitive data protection, secure configuration scanning, dark web monitoring, risk quantification and risk scores, industry comparison, compliance tracking, and a lot more.

The Vulnerability Scanning, Root Cause Analysis and Patching capabilities provided by the platform are enriched and enhanced by multiple other risk metrics. Organizations can both find vulnerabilities and understand the larger context that they are a part of, enabling granular assessment and a more informed mitigation strategy.

Network Discovery

CYRISMA Network Discovery (or asset discovery) scans can be set up to scan IP subnets and discover target machines. The results show all IP devices discovered, and the target machines with supported operating systems. These target lists can be easily merged into the system to scan them for vulnerabilities (as well as sensitive data and configuration weaknesses).

Vulnerability Scanning

The CYRISMA vulnerability scanner includes capabilities for internal, external, authenticated, unauthenticated, agentless and agent-based scans. Users can also patch Windows-based third-party applications from within the platform. The platform gives organizations complete visibility into the vulnerabilities in their network-connected devices, systems and web applications, and allows them to easily triage these vulnerabilities based on severity levels, create mitigation plans, and patch systems quickly.

Root Cause Analysis

CYRISMA users can drill down into the root causes of all vulnerabilities. Because multiple vulnerabilities can be associated with a single root cause, the ability to see these related CVEs grouped together simplifies prioritization and patching. In addition to listing CVEs based on root causes, the platform also displays the machines and systems impacted by each root cause.

Patch Management

The CYRISMA Patch Manager displays the root causes of the vulnerabilities found during scans and enables users to schedule patches to address these root causes and associated CVEs. Currently, the platform has the ability to directly deploy patches on Windows-based third-party applications. For other vulnerabilities, users can see detailed mitigation options and choose a remediation or mitigation strategy based on organizational context.

Vulnerability Management is just one of CYRISMA's many powerful capabilities, and along with scanning capabilities to assess secure configuration and find and classify sensitive data, gives organizations a comprehensive toolset to implement essential preventative and protective security controls.

Read more about platform capabilities and **watch a three-minute demo here**.