TLP:CLEAR

VULNERABILITY MANAGEMENT METHODOLOGY

IRM #21 CRITICAL VULNERABILITY PRIORITIZATION

Guidelines for the Cyber Threat Intelligence-based Critical Vulnerability Prioritization Process

IRM Author: Alex Kouzmine / CERT SG
Contributor: CERT aDvens
IRM version: 1.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

C'EST VOUS L'AVENIR

SOCIETE GENERALE

TLP:CLEAR

ABSTRACT

This Vulnerability Management Methodology (VMM) is a concise guide designed for professionals managing and addressing specific security vulnerabilities within an organization.

WHO SHOULD USE IRM SHEETS?

- System Administrators
- Security Operations Centre Teams
- CISOs and Their Deputies
- Vulnerability Management Teams
- Computer Emergency Response Teams

Key Reminders

Follow the IRM: Adhere to the established methodology to ensure a structured and effective approach to vulnerability management.

Document Thoroughly: Keep detailed notes of all findings, actions taken, and decisions made during the vulnerability assessment and remediation processes.

Keep Calm: Maintain calm and systematic procedures when identifying and addressing vulnerabilities.

Engage Appropriately: Contact your organization's Vulnerability Management team or CERT immediately if additional support or escalation is needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

By utilizing the Vulnerability Management Methodology sheets, organizations can ensure a consistent and efficient approach to identifying, prioritizing, and mitigating vulnerabilities. This structured methodology supports the protection of critical assets and enhances overall security posture.

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

OBJECTIVES:

Enhance Vulnerability Management

Improve the identification and prioritization of vulnerabilities through Cyber Threat Intelligence.

Optimize Resource Allocation

Ensure that limited resources are focused on addressing the most critical vulnerabilities.

Strengthen Incident Response

Integrate Cyber Threat Intelligence into Incident Response to provide context and actionable decision-making capabilities during incident handling.

Reduce Risk Exposure

Minimize the window of opportunities for attackers by proactively addressing high-risk vulnerabilities.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Develop or acquire vulnerability and exploit-related CTI sources such as threat feeds, intelligence reports, access to dedicated repositories and databases.
- Set up internal vulnerability monitoring & CTI tools and platforms for data aggregation and analysis.
- Assign responsibilities for CTI collection, analysis, and integration into vulnerability management.
- Create guidelines for vulnerability assessment and prioritization using CTI.
- Develop a comprehensive inventory of all systems and software versions within the organization to understand the potential attack surface.
- Establish a threat intelligence program to continuously gather and analyze data on emerging threats and vulnerabilities.
- Prepare communication channels and templates for rapid dissemination of information needed for Vulnerability Management purposes used during a vulnerability-related incident.
- Train the incident response team and other involved teams on the use of threat intelligence and vulnerability monitoring tools, services, and methodologies.
- Establish operational channels for efficient information sharing between involved teams.

Business Awareness for Proactive Vulnerability Management

Proactively managing vulnerabilities is crucial for safeguarding your business' information systems. Rather than waiting for an exploit to occur, **communicate the importance of vulnerability management to your organization**. Highlight relevant use cases to illustrate potential impacts on business operations and production, thereby drawing attention to the significance of timely vulnerability management. **Educate your stakeholders about what vulnerability management entails and make sure they understand the associated risks and benefits**. Make it clear that the stakeholders can reach out for help and assistance whenever needed. Through efficient awareness and open communication, you empower your teams in place to better protect your organization’s assets and information systems.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE APPROPRIATE PARTIES.

Vulnerability Scanning

- Use automated tools to identify vulnerabilities in systems and applications.

CTI Collection

Gather intelligence from various CTI sources, including open-source intelligence, commercial feeds, and information sharing and analysis centres, such as ISACs.

Threat Actor Profiling

- Identify potential threat actors relevant to the organization's industry and technology stack.

Vulnerability Scoring

- Evaluate the severity of identified vulnerabilities using standards like CVSS, EPSS, etc.

CTI Integration

- Correlate vulnerabilities with CTI to understand if they are being actively exploited or targeted by threat actors.

Environmental Analysis

- Assess the relevance of each vulnerability in the context of the organization's own environmental reality and realistic threat landscape.

Prioritization

- Determine the potential impact and likelihood of exploitation for each vulnerability.
- Apply CTI-derived scores to vulnerabilities based on factors like exploit availability, threat actor activity, and industry targeting.
- Create logic-based or scoring-based workflows to categorize vulnerabilities into priority levels (e.g. very high, high, medium, low) based on combined risk and CTI scores.
- Encompass the factor of business criticality and the potential impact on operations and production when prioritizing vulnerabilities for your organization.

Prioritization Standards & Tools

CVSS focuses on the **severity of vulnerabilities based on their technical characteristics** but lacks real-world exploitability data.

EPSS predicts the **likelihood of exploitation**, providing a more dynamic and actionable approach to **prioritization**.

Vulnerability Risk Management tools often combine CVSS and EPSS scores with additional organizational or environmental context, such as asset criticality or business impact.

Vendors & Organizations often develop their own Proprietary Scoring Models & Systems tailored to their specific risk tolerance and operational needs.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Develop action plans to address high-priority vulnerabilities first, leveraging patch management, configuration changes, or other mitigation strategies.
- Assign time-sensitive deadlines and service level agreements corresponding to the varying levels of vulnerability severity.
- Allocate resources effectively to ensure timely remediation of critical vulnerabilities.
- Inform relevant stakeholders about prioritized vulnerabilities and remediation plans.

A **Service Level Agreement** or **SLA** in Vulnerability Management is a **formalized agreement that defines the expectations, timelines, and responsibilities for addressing security vulnerabilities**. It is **essential for ensuring that vulnerabilities are remediated in a timely and efficient manner**, reducing the risk of exploitation and aligning with organizational security goals.

SLAs establish specific deadlines for fixing vulnerabilities based on their severity. For example, critical vulnerabilities might need to be addressed within 24 hours to 72 hours, while lower-risk issues could have longer timeframes. These timelines ensure that the most severe risks are prioritized and mitigated quickly.

SLAs are tailored to the organization's risk appetite and the potential impact of vulnerabilities. For instance, critical vulnerabilities that could lead to significant security incidents, dataleaks or downtimes are addressed more swiftly than minor issues.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

Remediation Planning

- Develop action plans to address high-priority vulnerabilities first, leveraging patch management, configuration changes, or other mitigation strategies.

Resource Allocation

- Allocate resources effectively to ensure timely remediation of critical vulnerabilities.

Communication

- Inform relevant stakeholders about prioritized vulnerabilities and remediation plans.

Establish Backup and Rollback Mechanisms

- Create system backups prior to applying patches or making changes; ensure systems or applications are backed up to allow for recovery in case of unexpected issues.
- Develop rollback plans and procedures to quickly revert changes if remediation actions trigger disruptions or fail to address the vulnerabilities effectively.

Conduct Pre-Remediation Testing

- Apply patches or configuration changes in a staging or sandbox environment to assess their impact before deploying in production.
- Proactively assess compatibility so as to make sure that the remediation actions do not negatively affect system performance, functionality, or compatibility with other applications.

Integrated Remediation Tracking Systems & Follow-Up Tools

By implementing remediation tracking and follow-up tools, organizations can transform vulnerability management from a cyclical process to a continuous improvement program, significantly enhancing the security posture while maintaining operational integrity across complex environments.

Remediation follow-up tools are specialized solutions that **track, validate and report on the effectiveness of vulnerability remediation efforts across an organization**. These tools bridge the gap between vulnerability management and patch management by providing continuous visibility into remediation progress and validating that security gaps are truly closed. When properly implemented, these systems create accountability, tangible visibility via dynamic KPIs and ensure no vulnerabilities remain unaddressed after initial remediation attempts.

Similarly, enterprise-wide remediation dashboards provide security teams and leadership with real-time visibility into remediation status, timelines, and effectiveness. These platforms consolidate data from various security tools to present a unified view of remediation progress against established SLAs and risk thresholds.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

Implement Remediation Actions

- For larger environments, consider rolling out the remediation actions in stages to monitor for issues and minimize risks - if applicable to your organizational structure and architecture.
- Use automation tools for tasks like patch deployment, configuration changes, or code updates to streamline the remediation process and reduce errors whenever possible.

Validate Remediation Effectiveness

- Conduct post-remediation tests to confirm that the vulnerability has been fully addressed without introducing new security issues or functionality problems.
- Use vulnerability scanning tools after remediation to make sure the previously identified issues no longer exist.

Documentation & Metrics

- Record all remediation activities, including undertaken actions and their respective outcomes.
- Track key performance indicators to evaluate the process' effectiveness.

Post-Remediation Processes & Services

Effective post-remediation processes incorporate verification testing that confirms vulnerabilities are truly resolved rather than superficially addressed. **Threat Hunting may be used in post-remediation context as a proactive security approach** that goes beyond traditional vulnerability scanning by actively searching for signs of adversary activity that may have occurred during the vulnerability's exposure window. TH may be seen as a critical verification layer that ensures environments remain secure after remediation actions. **TH employs advanced detection techniques including behavioral analysis, anomaly detection, and pattern recognition to identify potential compromise indicators** that standard vulnerability scanners might miss. For example, while a critical RCE vulnerability may be patched, threat hunting can reveal whether it was exploited prior to remediation by examining system logs, network traffic patterns, and file integrity changes.

Attack Surface Management or ASM process provides continuous visibility into an organization's external and internal attack surfaces, helping security teams understand the context and potential impact of vulnerabilities across the enterprise. **ASM complements traditional vulnerability management by offering real-time insights into exposure levels even after remediation efforts**. **ASM services continuously discover and inventory assets, monitor for changes to the attack surface, and provide prioritization capabilities based on business context and threat intelligence**. For instance, after remediating a critical vulnerability in a public-facing application, ASM can verify that the fix is correctly deployed across all instances and alert to any new deployments that might reintroduce the vulnerability.

LESSONS LEARNED

OBJECTIVE: IMPROVE FUTURE INCIDENT RESPONSE AND VULNERABILITY MANAGEMENT PROCESSES.

- Analyze the effectiveness of the vulnerability prioritization and remediation processes.
- Incorporate insights from the review into the CTI and IRM processes to improve future vulnerability management.
- Update policies, procedures, and tools based on lessons learned to enhance the overall vulnerability management lifecycle.
- Conduct a post-incident review to evaluate the effectiveness of the response and identify areas for improvement.
- Update threat intelligence and vulnerability management processes based on lessons learned.
- Share insights and findings with relevant stakeholders to enhance organizational awareness and preparedness.
- Compile a detailed report of the incident, including the vulnerabilities identified, actions taken, and outcomes achieved.
- Use threat intelligence to provide context and analysis of the incident, highlighting trends and patterns.
- Distribute the report to key stakeholders and use it to inform future threat intelligence and incident response strategies.

Knowledge Retention and Continuous Improvement

Knowledge Management in vulnerability response represents a critical component for building organizational resilience and preventing the recurrence of effective exploitation. Valuable knowledge often becomes trapped in isolated environments, preventing true organizational learning and leading to repeated security mistakes. Effective knowledge management transforms individual experiences into institutional wisdom by systematically capturing remediation approaches, mitigation strategies, and decision-making processes that worked—or didn't work—during security incidents.

Systematic collection and analysis of lessons learned during vulnerability remediation creates a feedback loop that continuously strengthens an organization's security posture. By documenting near misses, successful mitigations, and remediation challenges, security teams build an institutional memory that becomes increasingly valuable over time. This knowledge repository allows organizations to highlight averted security incidents thus quantifying the "non-events" that represent successful security interventions, which helps demonstrate the value of security investments and proactive remediation efforts to leadership.