Office of the Chief Information Security Officer

Vulnerability management guidelines

Last updated: Jan. 22, 2024

UNIVERSITY OF TORONTO

Contents

UNIVERSITY OF TORONTO

1. Preamble

Cyber security is a high-stakes race with cyber defence teams continuously working towards identifying and patching system vulnerabilities before they can be exploited. These vulnerabilities are inevitable as organizations digitize operations with advancing technology and cloud adoption.

Vulnerability management is a process by which identified vulnerabilities are tracked, evaluated, prioritized and managed until the vulnerabilities are remediated or otherwise appropriately resolved. Managing the identified vulnerabilities ensures that appropriate actions are taken to reduce the potential that these vulnerabilities are exploited, and thereby reduce the risk of compromise to the confidentiality, integrity and availability of information assets.

By applying updates at an interval, the expected result is reduced effort dealing with exploits by eliminating or reducing the related vulnerability. Effectively managing vulnerabilities is a continuous activity, requiring focus of time, attention and resources. This standard defines the requirements for notification, application of security-related patches and procedures for vulnerability management.

2. Scope and applicability

The guidelines apply to all University of Toronto-managed information technology systems (servers, workstations, network devices, databases, applications and end points) that enable and support U of T operations.

The goal of these guidelines is to provide units with a framework for developing their own vulnerability management process.

3. Policy

To ensure the confidentiality, integrity and availability of information and information systems at the University, information security controls must be in place for the use of all University-owned technologies in accordance with the U of T's Information Security and the Protection of Digital Assets Policy.

The vulnerability management guidelines are written consistent with the University's Information Security Control Standard and the Information Security and the Protection of Digital Assets Policy.

UNIVERSITY OF TORONTO

4. Vulnerability management

4.1 Vulnerability assessment

Vulnerability assessment (VA) is the process of identifying security vulnerabilities across information systems. The results of the assessment provide security teams and stakeholders with the information they need to analyse and prioritize vulnerabilities for remediation.

Vulnerability assessment tools exist in many forms. Most importantly, these tools should be able to:

- Scale to include various types of assets.
- Establish a baseline metric to determine changes over time.
- Identify and report on the security configuration of IT assets.
- Discover unmanaged or unknown assets on networks.
- Produce reports with regards to compliance gaps.
- Provide risk assessment and remediation priorities.
- Provide recommendations on how to update and remediate issues.

Types of monitoring tools and processes

Observational:
Most basic type of monitoring that is used to review hardware and software to report on their operational efficiency and effectiveness.

Analysis:
These tools and processes take observational data and analyse it further to determine origin, why problems are occurring, and potentially predict when problems might arise.

Engagement:
Leverage both observational and analysis tools and processes to determine how to act upon this information. They can range from service tickets being created, certain team members being informed, additional services added, or systems restarted or stopped.

Emerging threat monitoring:
Review of bulletins and vendor notices to evaluate indicators, presence or likelihood of risks.

Types of scanning

Network:
Most widely used and performed remotely to all network attached assets. These can be run both as authenticated or unauthenticated scans.

Agent:
Resides on scan targets and runs in a persistent state to collect information in real time. Used to perform scans on targets that cannot be done remotely.

Passive:
Used for assets that are sensitive to active scanning. However, due to the sensitivity of these systems, a complete list of vulnerabilities may not be delivered from these scans.

Web app probe:
Tool that detects, discovers, and catalogues web applications and APIs. These scans comprehensively and accurately detect the presence of misconfiguration, cross site scripting, vulnerabilities, data leaks and presence of malware.

Source code review:
Analyse source code or compiled code to determine vulnerabilities.

Teams should consider the following asset types for monitoring and scanning:

- Applications
- Storage devices
- Servers
- Network devices
- Security devices
- Workstations (including laptops)
- Mobile devices (including tablets)
- Anything with an IP (internet of things devices)

Guidelines

- Monitor security sources for vulnerabilities, patch releases, non-patch remediation and emerging threats.
- Perform scans during the development cycle to assess the status of applications and infrastructure for known vulnerabilities.

- When scanning using a cloud-based product, review your policies and standards to determine whether the location for storing vulnerability scans data aligns with policy requirements.
- Run your scans ideally once a week, but at least once a month. If there are standards outlined at the University or your unit, those established standards should take precedence over this recommendation.
- If the asset cannot be scanned, an exception should be made that has been accepted and acknowledged by your leadership.

Supporting standards

- System & information integrity
- Risk assessment
- Security assessment

What is available at the institutional level at U of T?

Scanning**:**

- Network scans
- Agent-based
- Agentless credential-based solutions are currently under review

See Vulnerability Management Services available at the institutional level.

4.2 Vulnerability prioritization

With the ever-expanding threat landscape, it is not possible to remediate all vulnerabilities as they are discovered, so it is important to focus on the vulnerabilities that pose the most risk. This is accomplished through vulnerability prioritization: ranking and attacking risks based on potential impact to the business.

Guidelines

Assess vulnerabilities for the risk posed to assets and infrastructure considering the following factors:

- Vulnerability impact as indicated through the Common Vulnerability Scoring System (CVSS) or equivalent scores)
- Threat likelihood (availability of exploit, scale of asset exposure)
- Asset value

Based on the analysis, assign a risk rating (i.e., low, medium, high, critical) to the vulnerability, which will determine the recommended timeframe for remediation per the following table:

Risk rating	CVSS score (or equivalent)*	Nominal asset	Critical digital asset
Low	< 4.0	Based on resource availability	Based on resource availability
Medium	4.0 - 6.9	No longer than nine months	No longer than six months
High	7.0 - 8.9	Within three months or sooner	Within one month or sooner
Critical	9.0+	As soon as possible (recommended within seven-14 days)	As soon as possible (recommended: within 24-72 hours)

Table: Vulnerability remediation timelines

*Use the CVSS score thresholds for risk rating unless mitigating controls such as reduced exposure has been documented and implemented.

Emergency circumstances

In an emergency circumstance where a vulnerability is widely exploitable, it might be necessary to block or suspend a service at short notice until the vulnerability is remediated. If the unit fails to take timely action, the Chief Information Security Officer (CISO) may exercise emergency powers under the Information Security and the Protection of Digital Assets Policy.

4.3 Action on vulnerability

Once vulnerabilities have been identified and prioritized, the next step is to act on them to ensure the risk is appropriately managed.

Guidelines

- Ensure a plan is in place for addressing the identified vulnerabilities. This involves taking one of the following actions:
    - Determine the vulnerability is a false positive.
    - Remediate or eliminate the vulnerability per the defined timeline.
    - Mitigate the vulnerability using compensating controls.
    - For vulnerabilities that cannot be remediated, formally accept the risk or suspend service.

- Generate periodic reports to inform leadership (e.g., IT directors, chief administrative officers, principal/deans, CISO) on vulnerability management risk.
- Ensure there is a unit-specific vulnerability response playbook.

Additional guidance on building relevant processes

Process for vulnerability remediation:
Implement an asset and patch management process to keep all software up to date. Where possible, use centralized and automated tools to help with the identification and application of software updates, as well as mitigation steps for unsupported and end-of-life software and firmware.

- Maintain a database of patches.
- Oversee patch distribution, including verifying that a change control procedure is being followed. Use an automated centralized patch management distribution tool, whenever technically feasible.
- Before applying a patch and/or remediation, test them for stability and impact to the asset.
- Deploy the patch and/or non-patch remediation.
- Ensure any expected service interruptions are communicated in advance.
- Follow the standard change management procedures and complete required restarts.
- Verify installation of patches and/or remediation.
- Communicate completion including any encountered exceptions.

Process for risk acceptance:
Develop a process for formally accepting risk associated with open vulnerabilities. This may include vulnerabilities that cannot be remediated or vulnerabilities that need more time for remediation.

- Submit the request to the IT and/or administrative leader for review, along with information on why the vulnerability cannot be remediated within the stipulated timeframe.
- On a periodic basis, or when the risk situation has changed, report accepted risk for critical and high vulnerabilities to the unit leader (e.g., deans, chairs or principals), business owner (if different from the unit leader) and the CISO where applicable. The unit leader decides whether the risk can be accepted. The decision should be logged and tracked in the risk register.
- Review accepted risks periodically, or when the risk situation has changed, to determine if they continue to be valid. If the vulnerability still cannot be remediated, the risk acceptance period should be formally extended.

4.4 Reassessment

The reassessment phase allows you to analyse if the pre-determined actions to address the vulnerability have been successful or if additional work is required to address new issues that may have arisen.

Guidelines

Conduct validation after the vulnerability is fixed or a control is implemented to ensure that it was successful and has not resulted in any new risk. VA tool scans, reports from configuration management tools or targeted penetration testing can be used for validation.

4.5 Continuous improvement

The continuous improvement phase seeks to measure the performance of the program to date while identifying ways to improve maturity. Metrics used to measure performance should focus on the identifying trends in the security posture, effectiveness of removing vulnerabilities by asset, and measure performance of the process itself (e.g., discovery to remediation time).

The process can be simple to meet the department needs.

Guidelines

- Identify metrics for evaluating the effectiveness of the Vulnerability Management Program.
- Analyse data on an ongoing basis to identify trends and underlying causes of security issues such as particular products, organizational units or processes.
- Develop a process for assigning identified improvements to reduce underlying risks, where appropriate, based on a cost-benefit analysis.
- Develop a process for evolving metrics so that irrelevant metrics can be retired over time and new ones can be identified.
- As processes improve, update remediation targets to ensure balance between the goals of the institution and the risk appetite of the institution.

5. Roles & responsibilities

The following table outlines the key responsibilities for implementing the vulnerability management program.

Role	Responsibilities
ITS Information Security	• Send out communication about critical vulnerabilities with a known exploit • Provide institutional capability for scanning and reporting on vulnerabilities • Provide subject matter expertise to units

Office of the CISO	• Approve and release policy/guidelines on vulnerability management
ISC Working Group	• Develop policy/guidelines on vulnerability management
Divisional/unit leadership	• Provide resources for executing vulnerability management plans • Provide support for ongoing vulnerability management plans • Risk acceptance and acknowledgement • Review reports and dashboards to understand the state of all assets
Asset owners*	• Ensure assets are monitored and scanned or there is a valid exception in place • Ensure appropriate resources are available to remediate vulnerabilities as per guidelines • Ensure identified vulnerabilities are addressed within the recommended timeframes • Plan vulnerability scans to minimize impact on operations
IT team	• Manage day-to-day operation of VM plan

*Asset owners can be IT teams who manage assets on behalf of units, or individuals who might own and/or manage their own digital assets.