McMaster University

University Information Security Standard

Complete Title:
Vulnerability Management Standard

Standard Number (if applicable):
IS-12-VULN

Approved by:
Chief Information Officer

Date of Most Recent Approval: (annual review)

Date of Original Approval(s):

Supersedes/Amends Policy dated:
n/a

Responsible Executive:
Chief Information Officer

Enquiries:
IT Security (c-it-security@mcmaster.ca)

DISCLAIMER: *If there is a discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*

TABLE OF CONTENTS

VULNERABILITY MANAGEMENT STANDARD

INTRODUCTION

Errors made during software development, as well as implementation and configuration errors, lead to vulnerabilities that increase the risk of compromise to computing resources. Vulnerable resources may be exploited resulting in the loss of intellectual property, personal information, or denial of service.

Resource owners are responsible for ensuring that the resources for which they are responsible are configured securely and maintained to limit the exposure from potential vulnerabilities. It is the owners' responsibility to ensure that their resources are maintained by an experienced and qualified technical specialist to manage the risk of vulnerabilities appropriately.

Purpose

1. The purpose of this document is to establish the responsibilities and communication protocol for the treatment of risk related to vulnerable computing resources connected to the University data and telephony networks.

Scope

2. Compliance to the standards within this document is required for all high risk servers, where either the likelihood or impact of an incident is elevated, including:

    a) Servers that are accessible from the public network (internet);

    b) Servers that collect credentials to authenticate people, and particularly those that leverage the centralized authentication services (single-sign-on);

    c) Servers that handle credit card transactions, or are considered to be in scope for PCI-DSS compliance;

    d) Servers that are used to collect or handle personally identifiable information (PII), personal health information (PHI), or any other information classified as confidential or restricted according to the ***Information Classification Matrix***.

e) Servers that provide or support communication and collaboration services, including electronic mail.

3. Compliance to the standards within this document is recommended for all other servers that are connected directly to the University data and telephony networks, as well as all other computing resources owned by, operated by, or operated on behalf of the University.

Definitions

4. A **computing resource** is any type of computer that is connected to the University data or telephony network. This includes but is not limited to servers, workstations, laptops, mobile devices, network appliances, telecommunication and teleconferencing devices, printers, automation hardware, and industrial control systems.

5. A **public facing** resource accepts anonymous connection requests from any public internet protocol address. An **externally accessible** resource accepts connection requests from trusted external internet protocol addresses. Public facing and externally accessible resources have been included in the perimeter network access control list to allow these connections. An **internal** resource accepts connection requests only from other computers on the University network.

6. The **service owner** is the department head who is accountable for the service, and computing resources required to provide the service, within the organization. A **technical specialist** is an individual or team to whom the service owner has delegated the responsibility for configuring and maintaining the computing resources upon which the service is offered.

7. A complete glossary of definitions can be found in the ***Information Security Glossary***.

VULNERABILITY MANAGEMENT

8. Service Owners are accountable to the University for risk related to vulnerabilities on the servers that support their service. Service Owners, and their delegated Technical Specialists, are responsible for ensuring that their computing resources are configured in compliance with University technical standards, including but not limited to the ***Server Security Standard*** and the ***Client Computing Devices Security Standard***, and are appropriately protected according to the monetary value of the device and / or the classification of information stored on or processed by the server.

9. The University is authorized to test all computing resources that are connected to the University network, as well as any resource hosted on another network on behalf of the University, in order to discover and assess vulnerabilities, and to audit computing resources for compliance to University standards.

10. Vulnerability risk is assessed based on the likelihood and impact of the vulnerability being exploited. Factors affecting vulnerability risk include, but are not limited to:

    a) Vulnerability score assessed using the ***Common Vulnerability Scoring System (CVSS)***;

    b) Availability of an exploit for the assessed vulnerabilities;

    c) Resource specific network access controls;

    d) The purpose or function of the computing resource, including the sensitivity and/or confidentiality of the data hosted or processed by the resource.

    e) Age and supportability of the computing resource, including hardware and software.

    f) Any other compensating control or mitigating factors that reduces the risk of exploit.

11. Risks that result from vulnerabilities on computing resources must be treated within an acceptable time frame as determined by the University, in cooperation with the resource owner. Failure to treat the risks within the agreed acceptable time frame may result in removal of the resource from the network.

12. Computing resources that are public facing, publically accessible, and other high-value resources, must pass vulnerability testing, and must be re-tested regularly due to the evolving nature of vulnerabilities. These include:

    f) Resources that are to be accessed from the public network (internet)

    g) Resources that leverage the centralized authentication services (single-sign-on)

    h) Resources that handle credit card transactions, or are considered to be in scope for PCI-DSS compliance

    Software for which support has been terminated by the vendor or development community is not suitable for the services listed above.

VULNERABILITY RISK MITIGATION STANDARD OPERATING PROCEDURE

13. The University will send vulnerability notifications to the resource owner, and the delegated technical specialist if one has been identified. The notification will contain the following information:

    a) An initial vulnerability risk assessment;

    b) Description of the vulnerability;

    c) Recommended action(s) to treat the risk;

    d) Acceptable time to treat the risk;

    e) Required time to acknowledge the notification; and,

    f) Supporting information, if available.

14. Vulnerability notifications may be raised to the appropriate Vice-President when they are found to increase risk on high profile public resources.

15. Service owners, server owners, or their delegated technical specialists must acknowledge receipt of the alert within the required time to respond. This acknowledgement must include:

    a) Action to be taken to treat the risk;

    b) Proposed date by which the risk will be treated. This date must fall within acceptable time to resolve. If the resource owner is able to identify compensating controls or mitigating factors that reduce risk, change to the acceptable time to resolve will be negotiated.

16. Failure to acknowledge the notification before the required time to respond, or failure to treat the risk before the acceptable time may result in the enforcement of access restrictions or removal from the network.