# Vulnerability Scanning and Remediation Process

**Version 2.2**

## PROCESS INFORMATION

*This table should be completed by the responsible office and ITS Risk & Compliance, as it provides general information about the process.*

| | |
|---|---|
| **RESPONSIBLE OFFICES** | IT Security Office |
| **RELATED DOCUMENTS** | ▪ Information Technology Security Standard |
| **REFERENCE DOCUMENTS** | ▪ NIST FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems<br>▪ Accessing Vulnerability Data in ITGRC |
| **DOCUMENT CONTROL NUMBER** | ITS.ITSO-PRS002 |
| **PURPOSE** | This document provides an overview of the process involved in network vulnerability scanning of Mason's server environment and their remediation. This document is for IT Security Office, University System/Application Administrators and University System Owners who manage or own server environments. |
| **LAST REVIEWED DATE** | 1/4/2024 |

## NOTE TO ALL USERS

Helper-text in white table cells bound by "< >" are designed to help the user with content. Once the user starts typing, the helper texts will automatically be written over and removed. Texts in table cells shaded gray are fixed and shouldn't be edited.

## REVISION HISTORY

| VERSION | DATE | ORGANIZATION/AUTHOR | DESCRIPTION OF CHANGES |
|---|---|---|---|
| 1.0 | 1/14/2018 | IT Security Office | Initial release |
| 1.01 | 1/22/2018 | IT Security Office | Changed Response Time in Section III.C to match business week cycle. |
| 1.02 | 7/19/2019 | IT Security Office | ▪ Added NIST FIPS Publication 199 in Related Law & Policy section and Section III.A.7<br>▪ Updated Section III.A.7 to address classification<br>▪ Added a graphic process flow diagram in Section II |
| 1.3 | 2/14/2020 | IT Security Office | ▪ Approved with No Changes<br>▪ Formatting change only – copied previous version onto updated ITS |

| VERSION | DATE | ORGANIZATION/AUTHOR | DESCRIPTION OF CHANGES |
|---|---|---|---|
| | | | Process Template and updated Version Number |
| 1.4 | 3/4/2020 | IT Security Office | Updated table in Section III.C by making a minor change to the column header name. |
| 1.5 | 3/17/2021 | IT Security Office | ▪ Reformatted content on version 1.3 of process template<br>▪ Included additional source under References<br>▪ Clarified paragraphs in Section I, Overview<br>▪ Clarified step 7 in Section III.A, Vulnerability Scanning<br>▪ Corrected grammar in Section III.C, Vulnerability Notification and Remediation via ITGRC<br>▪ Added clarification and corrected grammar in Section III.D, Exceptions and Non-compliance<br>▪ Clarified Section III.E, Reporting<br>▪ Deleted the approver line for CISO since that position no longer exists after the reorganization; Updated title in Section VII, Signatures |
| 2.0 | 9/2/2021 | IT Security Office | ▪ Updated Section III.A.7 to reflect the current process on vulnerability scanning<br>▪ Updated Section III.B to reflect the current process on vulnerability notification and remediation<br>▪ In the table in Section III.B, the language and timing have been updated<br>▪ Added a new Section III.C, Security Evaluation and this caused the remaining previous sections to move down<br>▪ Updated hyperlink to university policy in Section III.D, Exceptions and Non-Compliance<br>▪ Updated support information in Section III.F, Support |
| 2.1 | 10/24/2022 | IT Security Office | ▪ Document reformatting and updated Process Scope, Definitions, and Artifacts sections |
| 2.2 | 1/4/2024 | IT Security Office | ▪ Annual review with minor updates to the Remediation Steps table, Security Evaluation section, and Exceptions and Non-compliance section. |

## PROCESS SCOPE

*Describe the overall scope of the process. It is* ***concerned primarily with controlling who, what, or when this process is applicable.*** *Please consider this a high-level summary.*

**The process…**

This process provides university System/Application Administrators and System Owners with reporting of vulnerability(s) or control gaps and a response method.

**The process is applicable when:**

1. This process applies when a university System Owner or System Administrator decides to correct a problem, requests to use a mitigation plan, requests acceptance for identified vulnerability and control deficiencies, or reports a false positive or inaccurate finding for review.
2. This process also applies when the ITGRC system detects new assets.

## PROCESS INPUTS & OUTPUTS

*List/Describe the process inputs and outputs at high-level. Inputs are the resources it takes to complete this process successfully. Outputs are the final results that a successfully executed process would generate.*

**Process Inputs**

1. Service Request (SR) from Functional Offices for Network Vulnerability Scanning
2. IP Control for new serve networks
3. Discovery of existing serve networks during risk assessments with clients

**Process Outputs**

1. Request for Change to Network Operations
2. Email from IT Security Office (ITSO) Engineer to university system owners/administrators with tentative scanning schedules
3. Updated Tenable Asset List
4. Updated ITGRC application
5. ITGRC-generated list of identified vulnerabilities and corresponding remediation information
6. Vulnerability Treatment Plans
7. Vulnerability treatment events (if vulnerability is still present)
8. Approved Acceptance of Risks
9. Weekly scan results
10. Exemption Request
11. Monthly Reports

## DEFINITIONS

| ACRONYM/TERM | DEFINITION |
|---|---|
| CMDB | Change Management Database |
| IT GRC system | IT governance, risk, and compliance system |
| ITSM | IT Service Management |
| ITSO | IT Security Office |
| RFC | Request for Change |
| SR | Service Request |

## FLOWCHARTS

*The flowchart(s) provide a graphical representation of the <purpose of the process> flow.*

**Provide an image of a Visio diagram to show process steps.**

None

## HIGH-LEVEL PROCESS OR STEP

*Provide high-level process description along with the activity outputs for each process step.*

| PROCESS/STEP DESCRIPTION | Responsible Group | Output(s) |
|---|---|---|
| **Vulnerability Scanning**<br>Weekly discovery and vulnerability scans are performed against all identified networks that host system deemed to be servers. An automated process feeds this data into the ITGRC system and creates new assets and associated scan data with the new or existing assets. This process for adding a new network to the scope is defined in the steps below. | | |
| 1. ITSO Engineers and Analysts determine new serve networks via:<br>a. IT Service Management (ITSM) tool for new network requests from clients<br>b. IP Control for new serve networks<br>c. Discovery of existing serve networks during risk assessments with clients | ITSO Engineer and Analyst | possible new serve networks |
| 2. ITSO Engineers determine if the new serve networks are correctly configured for VRF scanning. | ITSO Engineer | correctly configured serve networks |
| 3. ITSO Engineers submit an RFC in Change Management Database (CMDB) to Network Operations for new networks to be added in | ITSO Engineer | RFC |

| | | |
|---|---|---|
| order to correct their configuration for virtual and forwarding (VRF) scanning. | | |
| 4. ITSO Engineers request that the University System Owners/Administrators of assets in the newly created network to allow any ingress rule in their systems' host-based firewalls for vulnerability scanner network. A tentative scanning schedule is communicated via email. | ITSO Engineer | Tentative scanning schedule |
| 5. ITSO Engineers add the new networks to Tenable Asset Lists and set-up automatic/scheduled scans (if one does not already exist for the group or department). | ITSO Engineer | updated Tenable Asset List |
| 6. New asset entries are created in the ITGRC application in an automated fashion with the vulnerability data from Tenable Security Center. | ITSO | updated asset entries |
| 7. ITSO identifies the System Owner and directs the System Owner to assign the asset to a System Administrator. ITSO classifies the system with the help of University System/Application Administrators. The classification is based on the "high water mark"; e.g., if any of the three (Confidentiality, Integrity, or Availability) is rated High, then the system is classified as High. Refer to NIST FISPS PUB 199. | ITSO | Assigned System Administrator, risk classification |
| **PROCESS/STEP DESCRIPTION** | **Responsible Group** | **Output(s)** |

**Vulnerability Notification and Remediation via ITGRC**

Before initiating the vulnerability treatment process, ITSO performs a training session with University System Administrators and University System Owners that includes documentation on how to use the application and requirements for reviewing and responding to vulnerability treatment events. ITGRC application notifies and provides administrators with a list of identified vulnerabilities and corresponding remediation information. Refer to the System Administrator documentation in SharePoint for System Administrator step-by-step documentation on using the IT GRC application.

The table below provides the remediation response action with an expected timeline of business days based on the vulnerability risk for University System Administrators and University System Owners.

| Remediation Steps | Critical & High-Risk Vulnerability Response Time (business days) | Medium or Lower Risk Vulnerability Response Time (business days) |
|---|---|---|
| 1. System Administrators or System Owners must confirm that the vulnerability exists and respond with an appropriate plan to address the vulnerability(s) or assert that it is a false positive. | 5 | 20 |

| | | |
|---|---|---|
| 2. System Administrators or System Ownersimplements the approved plan by executing the steps described in this procedure | 10 | 25 |
| 3. Remediation is validated by subsequent scans | | |

| | | |
|---|---|---|
| University system administrators or system owners can treat vulnerability and/or control gaps by:<br>▪ Remediating the vulnerability or control gap with the solution provided in the treatment event.<br>▪ Requesting for approval of the use of mitigation strategy to address the vulnerability or control gap.<br>▪ Requesting for approval of the acceptance of risk from their leadership. ITSO will review the request and come to a resolution.<br>▪ Providing evidence for review and approval that the identified vulnerability is a false positive via the treatment event.<br><br>** System administrators must wait until the next scheduled scan is completed to verify if the applied changes were successful in remediating the vulnerability. The vulnerability treatment event will display if the vulnerability is still present. ITSO may perform ad-hoc scans for vulnerabilities with a higher risk.* | System Administrator or System Owners | Treated or mitigate vulnerability/control gaps or approved acceptance of risk |
| **PROCESS/STEP DESCRIPTION** | **Responsible Group** | **Output(s)** |
| **Security Evaluation**<br>The IT GRC application will create weekly scan results and notify System Administrators of event requiring awareness or treatment. The following describes the steps for the to perform this step: | | |
| 1. ITSO Analysts will review vulnerability treatments submitted by System Administrators. | ITSO Analyst | reviewed vulnerability treatments |
| 2. ITSO Analysts assess the impact of each vulnerability on Mason based on system classification of Confidentiality, Integrity, and Availability. | ITSO Analyst | assessed vulnerability based on CIA |
| 3. ITSO Analysts analyze vulnerabilities based on the Common Vulnerability Scoring System (CVSS) score from the vulnerability scanner and the likelihood of exploitation. | ITSO Analyst | assessed vulnerability based on CVSS score |
| 4. ITSO Analysts will approve or deny treatment plans for vulnerabilities submitted by the system administrator. | ITSO Analyst | approved or rejected treatment plan |
| 5. ITSO Analysts will verify that the treatment was successful. | ITSO Analyst | verified successful treatment |

| PROCESS/STEP DESCRIPTION | Responsible Group | Output(s) |
|---|---|---|
| **Exceptions and Non-Compliance** | | |
| 1. System Administrators must configure their systems to be open to scanning on all ports and protocols. If required, agent or authenticated scans must be supported to assess systems fully. If the University System Administrator or University System Owner believes that scanning is having a critical detrimental effect on a server, they can submit formal request for exemption.<br><br>A clear explanation and documentation must be presented to ITSO. ITSO will engage with leadership to approve or deny this request. | System Administrator | exemption request |
| 2. Failure to follow this procedure will lead to non-compliance with university policy, https://universitypolicy.gmu.edu/policies/information-technology-security-program/. ITSO may take the following actions:<br>a. Escalating treatment events to ITS or Distributed Space leadership<br>b. Removing the system from the Mason Network | ITSO | Escalation or removal of system from Mason network |
| **PROCESS/STEP DESCRIPTION** | **Responsible Group** | **Output(s)** |
| **Reporting** | | |
| ITSO Analysts generate a monthly report for University System Owners, System Administrators, and Leadership to summarize vulnerability treatment metrics. These include:<br><br>▪ Number of vulnerabilities reported for a department/service along with the severity<br>▪ Number of vulnerabilities remediated<br>▪ Time to remediate vulnerabilities (business days) | ITSO Analyst | monthly report |
| **PROCESS/STEP DESCRIPTION** | **Responsible Group** | **Output(s)** |
| **Support**<br>ITSO Analysts can be contacted at itsoanalyst@gmu.edu. | | |

## ARTIFACTS

*Provide a description of the artifacts referenced in this process.*

| ARTIFACT | PURPOSE |
|---|---|
| Acceptance of Risk | This is used to document, justify and formally accept risk for a known deficiency(ies). The leadership of the university system administrator or system owner is responsible for writing the justification and identifying the compensating control. |

| | |
|---|---|
| Exemption Request | The university system administrator or system owner submits this request to ITSO for an exemption from configuring their systems to be open to scanning on all ports and protocols. |
| Monthly Report | These reports are generated by ITSO for university system owners, system administrators, and leadership to summarize vulnerability treatment metrics. |
| Request for Change | The Request for Change is a formal request for the implementation of change. |
| Service Request | This is a formal request for service from a customer requesting for support, information, or some kind of action in the day-to-day operation of a business. |
| Tenable Asset List | This is a list of devices (for example, laptops, servers, tablets, or phones) within a Tenable.sc organization. |
| Treatment Event | These are vulnerabilities discovered in systems. |
| Treatment Plan | This is an approach the system administrators give ITSO Analyst to address treatment of vulnerabilities discovered in their system. |

## TIMETABLE FOR REVIEW

This process will be reviewed on as needed basis.

## APPROVALS

| ROLE | NAME & ORGANIZATION | SIGNATURE | DATE |
|---|---|---|---|
| IT Security Office Director | Curtis McNay | DocuSigned by: Curtis McNay 6179577EE174479... | 1/5/2024 |
| | | | |
| | | | |
| | | | |
| | | | |