Vulnerability Scanning, Assessment and Remediation Standard

Syracuse University – Information Technology and Services Information Security Standard – S0108

1.0 Scope

This standard covers any computing system connected to the Syracuse University (SU) wired network (with the exception of systems connected to the residence hall networks) including systems that are not owned and/or operated by SU.

2.0 Purpose

Improperly configured, outdated or unpatched computing systems can contain vulnerabilities that increase the risk of a successful compromise by attackers. Misconfigurations and vulnerabilities are often unknown to the administrators of these systems, or patching and updating of systems is given a lower priority to other tasks and projects. In an effort to identify and remediate these vulnerabilities, ITS has developed the following Vulnerability Scanning, Assessment and Remediation Standard.

3.0 Standard

SU's ITS Information Security Department (InfoSec) is responsible for operating and maintaining a vulnerability assessment and scanning program in accordance with SU's Information Security Framework control RA-05, and administrators of systems in scope of this standard are responsible for responding to scan reports as defined below.

ITS Information Security will:

1. Operate and maintain a vulnerability scanning platform for performing network based host discovery and vulnerability scans that will run against all systems in scope of this standard on a weekly basis, or after a significant change has been reported. Vendor updates to the vulnerability scanning tool will be checked for and applied before each scan. Since April 2013, the platform has been an integration of locally developed scripts and databases and the commercial tool.
2. Operate and maintain a web application scanning system for performing web application vulnerability scans that will run against all systems in scope of this standard on at least a quarterly basis, or after a significant change has been reported. Updates to the scanning tool will be checked for and applied before each scan. The system is currently an integration of locally developed scripts and the commercial tool.
3. Perform ad hoc scans as determined necessary by current threats and intelligence, on request of system administrators, or as needed for compliance needs.
4. Collect and analyze vulnerabilities discovered from items 1, 2 and 3.

5. Distribute discovered CRITICAL and HIGH vulnerabilities to known admins of systems within 1 business day of scan completion.
6. Track remediation of vulnerabilities, assess requests for extensions or exceptions, and manage reported false positives.
7. Provide a monthly report on all vulnerabilities to the Technology Leadership Council. This report will also be used to identify, monitor and address trends.
8. On request of University leadership, provide a report on all of the systems scanned, as well as all vulnerabilities tested for and discovered.
9. Escalate to management any critical or high vulnerabilities that are not addressed in a timely fashion (3 days for critical, 9 days for high *effectively 1 scan period for critical, 2 scan periods for high*).

System administrators of systems that are scanned under this standard will:

1. Configure any firewalls under their control to allow InfoSec to scan protected systems.
2. Review any scan reports provided by the InfoSec department.
3. Respond to high vulnerabilities within 9 business days or less (effectively 2 weekly scan periods).
4. Respond to critical vulnerabilities within 3 business days or less (effectively 1 weekly scan period).

"Response" can be any of the following actions:

- **Fix/Patch/Update:** Most vulnerabilities can be addresses by changing configurations, applying patches, updating code, or removing a system from the network. This is the preferred option and requires no additional interaction with InfoSec. When upgrading, older vulnerable versions of the software should be removed.
- **Report False Positive:** False positives can be addressed by sending an email to scanmaster@listserv.syr.edu that identifies the system, the vulnerability, and what you have done to determine that the finding is a false positive.
- **Request an extension:** Extensions may be requested when remediating the vulnerability within the required time frame is not possible due to resource limitations or business/academic impact. Extensions can be requested by creating an issue in the "Information Risk Assessment" (IRE) project on Orange Tracker. This in turn starts a workflow between InfoSec and the requester. The ISO or their designate will review all extension requests and may request additional information in order to assure that any risk is properly understood and addressed. Additional information on the workflow can be found in the **Risk Assessment and Exception Guideline – G0102.**
- **Request an exception:** Exceptions may be requested when remediating the vulnerability has a negative academic/business impact or for reasons that make it impractical. Exceptions may present greater risk to University and ***may*** require broader review and approval to include the ISO, CIO, or the appropriate dean, director, or department heads. Exceptions can be

requested by creating an issue in the "Information Risk Assessment" (IRE) project on Orange Tracker. This in turn starts a workflow between InfoSec and the requester. The ISO or their designate will review all extension requests and may request additional information in order to assure that any risk is properly understood and addressed. Additional information on the workflow can be found in the **Risk Assessment and Exception Guideline – G0102.**

4.0 Exceptions

- With the approval of the ISO, scans may be halted on any system or systems where the impact of the scans are causing an impact to business that cannot be corrected in any other manner.
- With the approval of the ISO, scans may be halted on the entire environment if there is a significant risk of business impact due to key business periods or lack or resources to address issues. Common times to halt scans are during change freeze periods and other identified times.
- As stated in the previous section, individual vulnerabilities may be granted exceptions from remediation by following **Risk Assessment and Exception Guideline – G0102.**

5.0 Referred Documents, Web Pages and Contact Information

Item	**Location/Info**
Guideline: Risk Assessment and Exception Guideline-G0102	http://its.syr.edu/infosec/docs/guidelines/RiskExceptionAssessmentGuideline-G0102.pdf
Contact: Information Security Officer	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.0
Effective Date:	March 21, 2016
Date of Last Review	June 1, 2017
Date of Next Mandatory Review	June 2, 2018