University of Connecticut

Information Security Office

Information Security Server Vulnerability Management Standards

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) / Page(s) Revised
6/1/2013	S. Gucwa	Initial Release	All
4/15/2015	M. DiGrazia	Updated Scheduling & Delivery Updated Exception Process	Page 5
5/10/2016	J. Pufahl	Updated Scheduling & Delivery	
11/15/2016	J. Pufahl	Document Review	All

Approvals

Review Date	Reviewed By	Name/Title	Action (Reviewed or Approved)
6/1/2013	RMAC	Risk Management Advisory Council	Approved
6/1/2013	CISO	Jason Pufahl, CISO	Approved
4/16/2015	CISO	Jason Pufahl, CISO	Approved
11/15/2016	CISO	Jason Pufahl, CISO	Approved

Table of Contents

Purpose

The purpose of the Server Vulnerability Management Standards is to establish the expectations and guidelines for applying service packs, hotfixes, and security patches (referred to generally as "security patches" throughout this document). In the interest of reducing the University's vulnerability exposure, the implementation of recommended configuration changes is also included within the scope of this document.

Definitions

Security patch – Code that will update the current version of a script or software, often used to fix a bug, update security, or add a new feature or new functionality (includes service packs, hotfixes, etc.).
Severity – This is the level of importance of the security patch as defined by the vendor.
Priority – This is the level of importance of the security patch as defined by UConn. This includes a timeframe for the expected installation of the security patch.
Data - Information collected, stored, transferred, or reported for any purpose in digital format. Data can include: financial transactions, lists, identifying information about people, projects or processes, and information in the form of reports. Because data has value and because it has various sensitivity classifications defined by federal law and state statute, it must be protected.

Scope

All servers on the University of Connecticut network.

Introduction

Security patches are updates to products to resolve a known issue or provide a workaround. Service packs update systems to the most current code base. Being on the current code base is important because that's where the operating system support focuses on fixing problems. Individual hotfixes and security patches should be adopted on a case-by-case, "as-needed" basis. They may or may not be relevant to a server installation. Evaluate the update, assess the risk of applying or not, and apply if appropriate.

The basic rules are:
The risk of implementing the service pack, hotfix, or security patch should ALWAYS be LESS than the risk of not implementing it.
And,
You should never be worse off by implementing a security patch. If you are unsure, then take steps to ensure that there is no doubt before moving changes into production.

Generic Best Practices

The items listed below are best practices that should be performed across all updates.

a. Use a change control process.

A good change control procedure has an identified owner, a path for customer input, an audit trail for any changes, a clear announcement and review period, testing procedures, and a well-understood back-out plan. Change control will manage the process from start to finish. Before applying any security patch, all relevant documentation should be reviewed.

b. Read all related documentation.

Reading all associated documentation is the first step in assessing whether the update is relevant and will resolve an existing issue; its adoption will not cause other issues resulting in a compromise of the production system; if there are dependencies relating to the update (i.e. certain features being enabled or disabled for the update to be effective); or, if potential issues may arise from the sequencing of an update. Specific instructions may state or recommend a sequence of events or updates to occur before the security patch is applied. Documentation released with the updates is usually in the form of web pages, attached Word documents and README.TXT files.

c. Testing

Testing, as appropriate, allows for "test driving" and eventual signing off of the update. Service packs and hotfixes should be tested on a representative non-production environment for critical or most impactful changes prior to being deployed to production.

If the update was tested by another service group at the University, and the testing parameters map adequately to the patch or service pack to be applied, assessing test results and deciding in favor of implementing the change based on tests performed by another admin or service team is acceptable.

d. Have a back-out plan, a working backup, and scheduled production downtime

A back-out plan ensures the system(s) and the University can return to their original state prior to a failed implementation. It is important that these procedures are clear, and that contingency management has tested them, since a faulty implementation can make it necessary to activate contingency options. The University may need to exercise the back-out plan in the event of the update not having an uninstall process or the uninstall process fails. The back-out plan can be as simple as restoring from tape or may involve many lengthy manual procedures.

As part of your back-out plan, it is recommended that you have a backup of your system.

e. Currency

Schedule periodic upgrades as part of standard operational maintenance and always be as current as possible with service packs/patch cycles.

Scheduling and Delivery

The application of security patches is scheduled to limit interference with users.

The required deployment schedule for security patches is as follows:

Critical/Emergency Security Patch	Remediated within 14 days
1-High	Remediated within 30 days
2-Medium	Remediated or accepted and documented in Nessus within 60 days (See Appendix A)
3-Low	Remediated or accepted and documented in Nessus within 60 days (See Appendix A)

The application of security patches for 3rd party vendor managed services is dependent on vendor SLA's. If the vendor cannot meet the University standards as laid out in this document, compensating controls should be considered.

Exceptions

If the application of security patches is not feasible, mitigating controls must be identified and implemented. The mitigating control(s) selected should be in proportion to the risk. If mitigating controls cannot be implemented, then an exception must be documented in Nessus. Instructions on how to review vulnerabilities and document decisions is located in Appendix A.

Responsibilities and Practices of the Information Security Office (ISO)

The ISO conducts scans of the University network resources to identify vulnerabilities. Only ISO or units approved by the ISO may conduct such scans. The ISO will create dashboards and ensure access is available to all IT staff managing servers or applications, as appropriate. The ISO may maintain logs of these vulnerabilities to identify patterns of behavior of concern.

Vulnerability Response Process and Responsibilities

When security vulnerability scans are completed, if ISO identifies vulnerabilities on a server or other resource connected to the network, the IT administrator or third party managing that resource will be notified of the apparent vulnerabilities so they can act accordingly to remediate them in accordance with the timeframe specified in this document.

Once notified of the vulnerable resource, the IT administrator or third party managing that resource should follow the schedule presented in the "Scheduling and Delivery" section to close the vulnerability. If a risk is accepted, this should be documented in Nessus within the remediation timeframe.

If the vulnerability is not remediated in the recommended or agreed upon timeframe and no exception has been granted, ISO staff may take necessary actions to safeguard the University network, including disconnecting the resource from the network to protect other computers and the integrity of the University computing environment. Detailed procedures for viewing vulnerabilities in Nessus and remediating/documenting risk actions is available in Appendix A.

Appendix A: How to Review Vulnerabilities and Document Decisions in Nessus

Overview

UConn's Information Security Office (ISO) is using a product called the Nessus Security Center Vulnerability Scanner, by Tenable Network Security, that will scan information technology resources for vulnerabilities, provide important information regarding security risks and aide IT security policy. The data from the scans are consolidated and centralized for review, remediation and documentation within the Security Center Management Console.

The ISO has pre-configured individual asset groups for each School, College or Department that administer servers or applications. We have done our best to be complete but are ultimately reliant on the infrastructure owners to ensure that the asset groups are accurate.

Access to the management console is available at https://nessus.uits.uconn.edu. This will enable you to view or add dashboards and interact with any vulnerabilities associated with IT infrastructure that you manage.

ISO Responsibilities

The ISO will ensure that asset groups are created and that the relevant IT staff are assigned appropriately to each asset group. It's our intention to provide you only with the information that is relevant to you. We will configure Nessus to scan your servers and applications for vulnerabilities on a weekly schedule. You will be able to review all current scan data at https://nessus.uits.uconn.edu. To ensure the most accurate scan results the ISO will update Nessus scanner plugins as Tenable releases or updates plugins.

Server/Application Administrator Responsibilities

Administrators are expected to utilize Nessus for vulnerability review, remediation and vulnerability management. The system provides a variety of dashboards that will enable you to review vulnerabilities at a high level, and drill down to review specific information at a host level. The system provides three options to manage specific vulnerabilities:

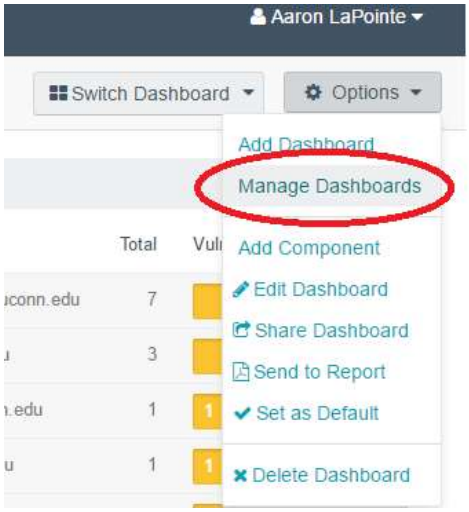
1. Launch Remediation Scan – This option assumes that you have made a change to your server/application that addresses the identified vulnerability. You can launch a remediation scan to ensure that the changes address this vulnerability. Alternatively, it is acceptable to wait until the next scheduled scan.
2. Accept Risk – This option allows you to document why you have chosen not to remediate the vulnerability identified. Common examples of when a risk may be accepted include (but are not limited to) the vulnerability being a false positive or other compensating controls in place that reduce the risk.
3. Recast Risk – This option allows you to modify a risk severity. Common examples of when a risk severity may be changed include, but are not limited to, the presence of compensating controls that reduce potential severity.

It is only our expectation that reasonable consideration is given to each vulnerability identified and that vulnerabilities are managed following the timeframe specified in the Server Vulnerability Management Standards. Vulnerabilities are expected to be remediated rather than accepted/recast whenever possible; but, it is also understood that legitimate reasons may exist for a decision to be made not to remediate a vulnerability.

Nessus Security Center Instructions

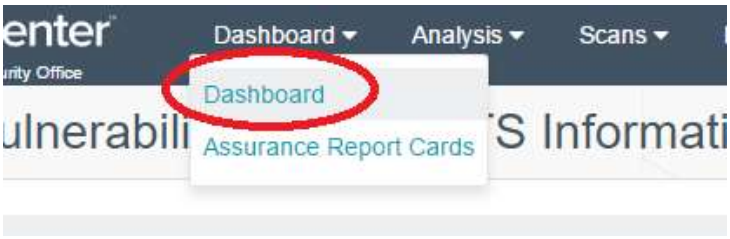
1. Go to https://nessus.uits.uconn.edu and log in with your NetID credentials.

2. **Manage and View your Dashboards**
   a. On the top right-hand side of the screen, click on "**Options**" and select "**Manage Dashboards**" from the drop down menu.

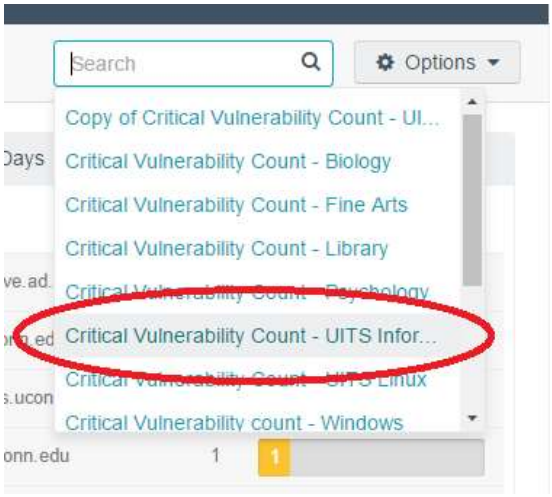


   b. Under "**Manage Dashboards"**, find the one that is relevant to your department. There should only be one labeled with your department.
   c. Notice how the pushpin is greyed out. Click it and it will turn blue and position as the others are.

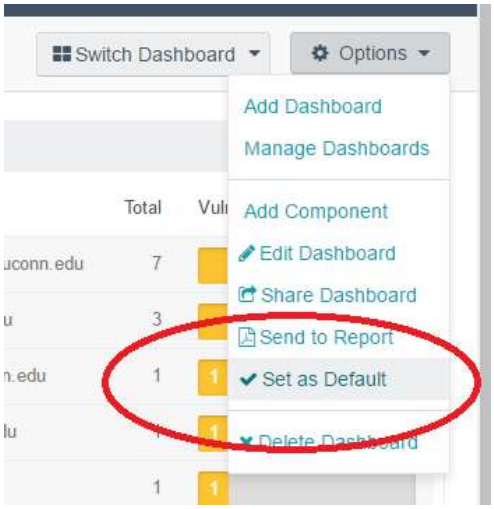
   d. At the top menu, select "**Dashboard**" to reveal a dropdown menu, then click on "**Dashboard**":



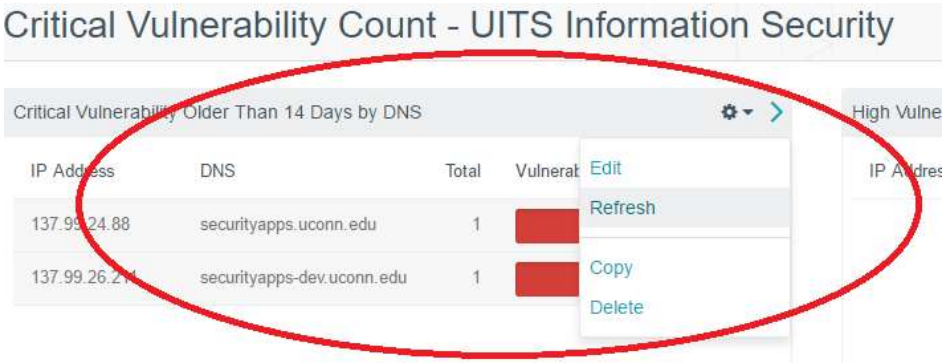
e. Again, on the top right-hand side of the screen, click on "**Switch Dashboards**", then select your dashboard from the pulldown menu:



f. To set this as your default dashboard, click on "**Options**" menu and then "**Set as Default**":

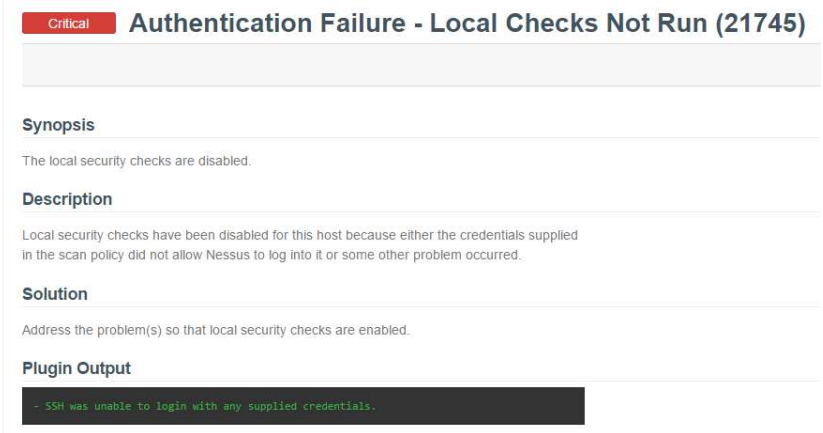


3. **To Refresh Data**
    a. Your dashboard is programmed to update once a day. You may need to refresh it to update your data. To do that, click on the gear of each pane and choose "**Refresh**".

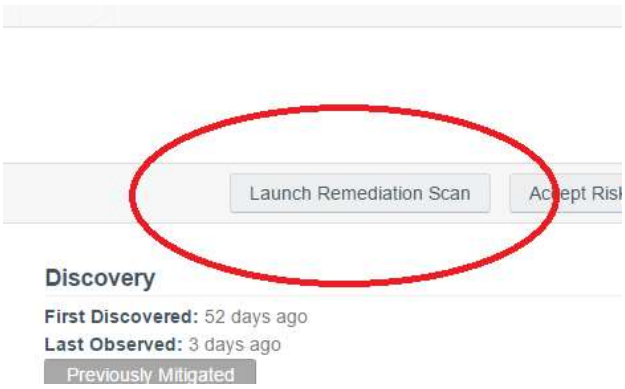


4. **To View/Remediate/Document Scan Results**
    a. The data contained in each of the panes should be fairly self-explanatory. The critical pane shows vulnerabilities that are out of compliance with UITS security policies, broken down by severity.

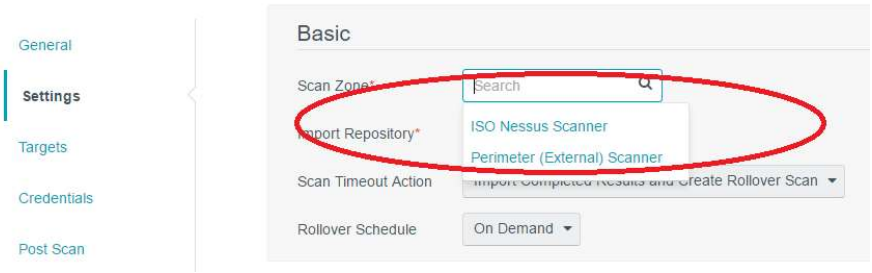
    b. To get details on a specific vulnerability, click on the light blue arrow in each pane and you will be able to drill down to the detail of each machine and vulnerability.
        i. Here is an example a vulnerability that is an authentication failure:



c. Once you have fixed an issue, you can perform a remediation scan that will check to see if the fix has been applied by clicking **"Launch Remediation Scan**":



i. In the wizard that you will be taken to next will have several menu options that must be populated.
   1. Under "**General**", there is nothing to do.
   2. Under "**Settings**", select "**ISO Nessus scanner**":



   3. Under "**Targets**", typically there is nothing to change. However if you had ten servers with the same vulnerability and you've fixed them all, it's possible to scan all the targets for that one particular vulnerability.
   4. Under "**Credentials",** you can manage which credentials should be used to scan your machines.
   5. The options under "**Post Scan**" are self-explanatory.
   6. Hit "**Submit**" to begin the scan.
   7. You will see the results of the scan under "**Scanned"** and then "**Scan Results**". If you've successfully mitigated your problem it will either be blank, or there may be some information shown here. If the vulnerability still exists, it will appear here now.