

Vulnerability Remediation Plugin Guide

ugin V 1.0 Doc Rev. 0.139

April 17, 2014

Table of Contents

Background 3 Purpose 3 PRE-REQUISITES 4 Supported versions of Venafi Trust Protection Platform 4 Venafi Updater & Screen Resolution 4 Required Rights 4 Required Configuration 4 INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 20 Introduction 20 Introduction 20 Introduction 20 Revoked 21 Renewed 21<	INTRODUCTION	
Purpose 3 PRE-REQUISITES 4 Supported versions of Venafi Trust Protection Platform 4 Venafi Updater & Screen Resolution 4 Required Rights 4 Required Configuration 4 INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority. 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Importing Results tot Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 20 Introduction 20 Introduction 20 Revoked 21 RepORTS 22 Scan Report 22 Scan Report 22 Scan Report 22 <th>Background</th> <th></th>	Background	
PRE-REQUISITES 4 Supported versions of Venafi Trust Protection Platform 4 Required Rights 4 Required Rights 4 Required Configuration 4 INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority. 10 Object Name 11 Application Type 11 NANAGING CERTIFICATE RESULTS 14 Inporting Result Details 14 Inporting Results into Policy Tree from Network Scan 16 Adding Results into Policy Tree from Network Scan 18 Reviewing Queue Details 18 Reviewing Queue Details 18 THE WORK QUEUE 18 Starting Work 20 Introduction 20 Introduction 20 Introduction 20 RepoRTS 22 Scan Report 22 Scan Report 22 Scan Report 2	Purpose	
PRE-REQUISITES 4 Supported versions of Venafi Trust Protection Platform 4 Venafi Updater & Screen Resolution 4 Required Rights 4 Required Configuration 4 INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results to Work Queue 17 THE WORK QUEUE 18 Rerewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Introduction 20 Revoked 21 Report 22 York Report 22 Scan Report 22 <tr< td=""><td></td><td></td></tr<>		
Supported versions of Venafi Trust Protection Platform 4 Venafi Updater & Screen Resolution. 4 Required Rights 4 Required Configuration 4 INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 NANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Reviewing Work 18 THE PORCESSING WINDOW 20 Introduction. 20 Revoked 21 Reported 21 Reported 21 Reported Sing WinDOW 20 Introduction. 20 Revoked 21 Report 22	PRE-REQUISITES	
Venafi Updater & Screen Resolution	Supported versions of Venafi Trust Protection Platform	4
Required Rights 4 Required Configuration 4 INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Importing Result Details 14 Importing Results to Vork Queue 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Starting Work 18 THE PORCESSING WINDOW 20 Introduction 20 Revoked 21 Report 22 Vork Report 22 Scan Report 22 TROUBLESHOOTING 23	Venafi Updater & Screen Resolution	4
Required Configuration 4 INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 Report 22 Work Report 22 Scan Report 22 Starting Work 21 Reports 22 Starting Report 22 Report 22	Required Rights	4
INSTALLATION 5 Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority. 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results to Vork Queue 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Reviewed 21 Renewed 21 Renewed 21 Renewed 21 Report 22 Vork Report 22 Scan Report 22 Starting Work 23	Required Configuration	4
Downloading the Plugin 5 Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results to Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Reviewed 21 Renewed 21 Reports 22 Work Report 22 Scan Report 22 Starting Report 22 Starting Work 21 Reports 22 Mork Report 22 Scan Report 22 Scan Report 22 </td <td>INSTALLATION</td> <td>5</td>	INSTALLATION	5
Installation Instructions 6 Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Revoked 21 Renewed 21 Report 22 Work Report 22 Scan Report 22 Starting Work 21 Report 22 TROUBLESHOOTING 22 Logging 23	Downloading the Plugin	
Accessing the Plugin 7 SEARCHING FOR CERTIFICATES 10 Certificate Authority. 10 Object Name. 11 Application Type. 11 Network Scan 12 MANAGING CERTIFICATE RESULTS. 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE. 18 Reviewing Queue Details. 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 IntroUBLESHOOTING 23 Logging 23	Installation Instructions	6
SEARCHING FOR CERTIFICATES	Accessing the Plugin	7
SEARCHING FOR CERTIFICATES 10 Certificate Authority 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 Reports 22 Work Report 22 Stan Report 22 TOUBLESHOOTING 23 Logging 23		
Certificate Authority. 10 Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	SEARCHING FOR CERTIFICATES	
Object Name 11 Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	Certificate Authority	
Application Type 11 Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 Reports 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23	Object Name	
Network Scan 12 MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE. 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed. 21 Reports 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	Application Type	
MANAGING CERTIFICATE RESULTS 14 Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Vork Report 22 Scan Report 22 Scan Report 22 Scan Report 23 Logging 23	Network Scan	
Reviewing Result Details 14 Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 Scan Report 22 Scan Report 23 Logging 23	MANAGING CERTIFICATE RESULTS	14
Importing Results into Policy Tree from Network Scan 16 Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23	Reviewing Result Details	
Adding Results to Work Queue 17 THE WORK QUEUE 18 Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23	Importing Results into Policy Tree from Network Scan	
THE WORK QUEUE.18Reviewing Queue Details18Removing Certificates from the Queue18Starting Work18THE PROCESSING WINDOW20Introduction20Queue20Revoked21Renewed21REPORTS22Work Report22Scan Report22TROUBLESHOOTING23Logging23	Adding Results to Work Queue	
Reviewing Queue Details 18 Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	THE WORK QUEUE	
Removing Certificates from the Queue 18 Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	Reviewing Queue Details	
Starting Work 18 THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23	Removing Certificates from the Queue	
THE PROCESSING WINDOW 20 Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	Starting Work	
Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	THE PROCESSING WINDOW	
Introduction 20 Queue 20 Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	Introduction	20
Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23		
Revoked 21 Renewed 21 REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	Queue	
REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	Renewed	
REPORTS 22 Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23		
Work Report 22 Scan Report 22 TROUBLESHOOTING 23 Logging 23	REPORTS	22
Scan Report 22 TROUBLESHOOTING 23 Logging 23	Work Report	22
TROUBLESHOOTING	Scan Report	22
Logging	TROUBLESHOOTING	
	Logging	23

INTRODUCTION

BACKGROUND

When enterprises discover new risks associated to certificates and private keys, security teams need to be able to detect, protect, and respond quickly and effectively.

PURPOSE

The Venafi TrustAuthority Vulnerability Remediation Plugin allows you to detect SSL certificates that may have been compromised as a result of the Heartbleed bug, weak signing algorithms, or low key strengths. In one bulk action customers can revoke and renew all compromised certificates and keys.

PRE-REQUISITES

SUPPORTED VERSIONS OF VENAFI TRUST PROTECTION PLATFORM

The Vulnerability Remediation Plugin requires one of the following versions of the Venafi Trust Protection Platform (formerly known as Venafi Encryption Director):

- 6.1.4
- 7.0.0
- 8.0.3
- 10.0.0
- 11.0.0
- 14.1.0

Although the Plugin may function properly on other versions of Venafi Trust Protection Platform, they have not been tested.

VENAFI UPDATER & SCREEN RESOLUTION

In order to install the Venafi Vulnerability Remediation Plugin, you must have a recent version of the Venafi Updater installed. Any version 2.0.6 and above is suitable for this Venafi Update Package.

The Plugin requires a minimum of 1280x1024 resolution on the screen.

REQUIRED RIGHTS

The Vulnerability Remediation Plugin is designed for Administrators of the Venafi Platform and requires the logged in user to have "Master Admin" rights assigned. Users with less rights may be able to run the Plugin, but they will likely receive errors during work processing. This is expected.

REQUIRED CONFIGURATION

In order for the Vulnerability Remediation Plugin to be able to bulk process the renewal of thousands of certificates at once, Venafi TrustAuthority SSL (formerly known as Venafi Certificate Manager) have the appropriate Certificate Authority Template (CA Template) objects configured and validated for use. Also, if the CA Template that you are using has required vendor specific fields, these fields must be able to be completed via policy so that certificates can be renewed in bulk. For information on configure CA Template objects, please view the section "Managing CA Templates" in the product documentation, available in your product's help menu, or downloadable for registered customers at https://support.venafi.com/forums/20697646.

Depending upon your version of Venafi Trust Protection Platform, in order to revoke certificates in bulk, certificates must already be configured and linked to the appropriate CA Template object. Venafi TrustAuthority 11 and 14.1 will attempt to determine the appropriate CA Template object from the policy tree, even if the certificate is not explicitly linked to it.

INSTALLATION

DOWNLOADING THE PLUGIN

The Vulnerability Remediation Plugin is available to download to all Venafi customers with a current maintenance contract. In order to download, you need to have a valid FTP Account for https://ftp.venafi.com. If you are an authorized Venafi contact for your organization and require an FTP Account, please email support@venafi.com to request a FTP account.

Download Instructions:

1. On a computer with internet access, open a web browser type https://ftp.venafi.com in your address bar.

(Note: depending upon your web browser the https may need to be typed in manually)

- 2. Locate the installation files for the version of Venafi Trust Protection Platform (formerly Venafi Encryption Director) where the plugin will be installed.
- 3. Locate the folder "Vulnerability Remediation Plugin" and click on the folder name



4. Click on the Zip file in the folder to start the download.

Note: The name of the zip file may vary from the example in the screenshot below

VENAFI.
 So Up Arrow Go Home O Upload + New Folder ✓ Rename Telete
Name 🔶
Vulnerability Remediation Plugin for 14.1.zip

5. Save the downloaded file to the location where you keep other Venafi Update Packages

INSTALLATION INSTRUCTIONS

1. Extract the contents of the *.zip file to the Venafi server on which you are installing the Plugin.

Note: If your production environment has multiple Venafi servers, it is only necessary to install the Plugin on one server.

- 2. Locate the *.vupkg file from within the extracted file contents. This is the Venafi Update Package.
- Copy the *.vupkg file to C:\Program Files\Venafi\Packages.
 Note: the location of "Venafi\Packages" may vary in your environment if you have installed the Venafi Trust Protection Platform to a custom location.
- 4. Click on the Start Menu.
- 5. Locate the "Venafi Updater" (formerly known as Director Updater).
- 6. Right click on Venafi Updater and "Run as administrator".

Notepad	•	
🥖 Venafi Updater 👩	Open	
Venafi Windows Administration Console	Pin to Unpin	administrator 6 Taskbar from Start Menu
Command Prompt	Remov	ve from this list
Manager	Proper	ties
Internet Explorer		Control Panel
SQL Server Management Studio		Devices and Printers
		Administrative Tools
		Help and Support
		Run
All Programs		Windows Security
Search programs and files	<u> </u>	Log off
🖉 Stage 🛃 🛃 🔀	0	S S S S S S S S S S S S S S S S S S S

Make sure your Windows Administrator Console (Win Admin) is closed.
 Note: it is not necessary to stop IIS or other Venafi services to install this plugin – only WinAdmin.

- 8. Locate and highlight the Venafi Vulnerability Remediation Plugin from the list of installable updates.
- 9. Click the Install button to start the installation of the plugin. Installation should only take a few seconds.



10. When installation is completed, the status bar in the lower left hand corner will say "Installation successful".



11. Close Venafi Updater.

ACCESSING THE PLUGIN

The Venafi Vulnerability Remediation Plugin is only available in the Windows Administration Console (WinAdmin). It is not available in the Web Administration Console (WebAdmin) or in Aperture.

The Plugin requires a minimum of 1280x1024 resolution on the screen. Please adjust your Remote Desktop session settings so that the remote window is in full screen.

- 1. Click on the Start Menu
- 2. Locate "Venafi Windows Administration Console"

3. Right click on "Venafi Windows Administration Console" and choose "Run as administrator"



4. Login as a Master Admin with your username and password

Login	
VENAFL Venafi Encry	version 14.1
	Username: aaron.hixson Password:
	<u>C</u> ancel <u>L</u> ogin

5. Once the Windows Administration Console loads, click on the Wizards menu.

6. Click on the "Bulk Renewals & Revocation" item from the Wizards menu



7. The Venafi Vulnerability Remediation Plugin will load. It is recommended that you maximize the Plugin window to take up the full remote session screen.

SEARCHING FOR CERTIFICATES

The left panel of the Plugin is your search configuration panel. It allows you select from building your bulk renewal job in four different ways. You can build your job by searching via Certificate Authority, Object name, Application object type, or by a Network Scan.

Making changes to search settings will clear your current results. As you perform searches for certificates, results will appear in the middle panel for you to review. Make sure you select your desired certificates from the Results (middle) panel and add them to your Work Queue (left) panel before making changes to your search settings.

CERTIFICATE AUTHORITY

The Certificate Authority search will allow you to locate certificates in your Policy tree by the CA template the certificate is associated with.

- Bulk Certificate Management

 File Reports

 Search

 Certificates issued by CA:

 Find

 Prind

 Object Name

 Object Name

 Application Type

 Network Scan
- 1. Click on the *ellipses* button (picture below)
- 2. Select the CA Template that you want to use for renewing certificates and click "Select".

Select	Configuration Object		×
Search	for:	2	
	Certificate Authorities Administrator Certificate Authorities Internal SSL (1-Year SHA256) Certificates Lab 11 - Secure & Protect		
	<u>C</u> ancel <u>S</u> ele	ect	

3. Click on the "Find" button to search the Policy tree for all certificates that are linked to the selected CA Template object

🔑 Search	*
Certificates issued by CA:	
\VED\Policy\Administrator\Certificate Auth	
P Find	

OBJECT NAME

Selecting "Object Name" gives you the ability to type in a name and search for certificates by certificate object name, device object name, or application object name.

- 1. Click on "Object Name"
- 2. Type in the name of the object you'd like to search for
- 3. Click the "Find" button

🔑 Search	~
Search for:	
travel	
Found 17 certificates matching 'travel'	

4. The total count of found certificates will appear below the search controls. Results will appear in the middle Results panel.

APPLICATION TYPE

Selecting "Application Type" allows you to search for certificates in the policy tree by the type of associated application object.

- 1. Click on "Application Type"
- Use the CTRL or SHIFT key to select multiple application objects.
 Quick Tip: Click the top application object and use the SHIFT key to select the last application object to select all available options.

3. Click the "Find" button

Search for: A10 AX Traffic Manager Apache Basic Brocade CAPI Cisco ACE Cisco CSS CiscoCSM DataPower Find Found 5 certificates matching Apache or IIS 6	🔑 Search	*
A10 AX Traffic Manager Apache Basic Brocade CAPI Cisco ACE Cisco CSS CiscoCSM DataPower ✓ Find Found 5 certificates matching Apache or IIS 6	Search for:	
Apache Basic Brocade CAPI Cisco ACE Cisco CSS CiscoCSM DataPower	A10 AX Traffic Manager	
Basic Brocade CAPI Cisco ACE Cisco CSS Cisco CSS Cisco CSM DataPower	Apache	
Brocade CAPI Cisco ACE Cisco CSS Cisco CSM DataPower	Basic	
CAPI Cisco ACE Cisco CSS CiscoCSM DataPower Find Found 5 certificates matching Apache or IIS 6	Brocade	
Cisco ACE Cisco CSS CiscoCSM DataPower	CAPI	
Cisco CSS CiscoCSM DataPower	Cisco ACE	
CiscoCSM DataPower Find Found 5 certificates matching Apache or IIS 6	Cisco CSS	
DataPower Find	CiscoCSM	
Find Found 5 certificates matching Apache or IIS 6	DataPower	-
Found 5 certificates matching Apache or IIS 6		🔑 Find
	Found 5 certificates matching	Apache or IIS 6

4. The total count of found certificates will appear below the search controls. Results will appear in the middle Results panel.

Note: If certificates are associated to multiple application objects (one-to-many) than the certificates may be counted more than once. The list of unique certificates, however will appear in the middle Results pane.

NETWORK SCAN

The Venafi Vulnerability Remediation Plugin has the ability to scan the network for Heartbleed vulnerabilities, insecure hashing algorithms, and low key strengths to discover where security vulnerabilities may lie both in your internal and public networks.

Scan Existing Devices

Choosing "Scan existing devices" will utilize the host address on application objects and network validation settings on application and certificate objects to provide a list of IP Addresses and ports to scan to detect vulnerable private keys and certificates.

Note: Certificate objects that have network validation settings to "Use Subject Common Name" will not be included in the discovery job when "Scan existing devices" is selected.

🔑 Search		«
Scan existing de	vices	
Scan address rar	nge:	
Start Address:	10.10.10.1	
End Address:	10.10.30.255	
Ports:	443,8443	
Only add items ma Heartbleed V Insecure Hash Low Key Strend 	utching these criteria: ulnerability Detected ning Algorithms [MD5, SHA1] ngth [< 2048 bit] Start Scan	

Scan Address Range

If you select "Scan address range" you can provide one IP address as well as list the ports to scan.

Note: Ports need to be in a comma separated format. Separating ports by semicolons will not work.

Vulnerability Criteria

Heartbleed vulnerability: This will detect servers that have not been patched and still have an affected version of OpenSSL providing TLS sessions.

Insecure Hashing Algorithms: This will detect certificates that are using SHA1 or MD5 as their signing algorithm.

Low Key Strength: This will find certificates that have a private key less than 2048-bits

If none of these three vulnerabilities are checked, then the middle Results panel will be populated with any certificate found during the network scan.

Running the Scan

While the scan is running, there is a detailed status of its progress.

Start Scan	Network Scan 🛛 🛛 🛛
12033 ports scanned, 524 connections succeeded, 11509 connections failed	Please wait while your network scan is running Waiting for 420 threads to complete
	Cancel

Scan Report

Network Scan results can be exported so that vulnerable servers can be patched prior to rotating the certificate and private key. See the Reports section for more information on the Scan Report.

MANAGING CERTIFICATE RESULTS

REVIEWING RESULT DETAILS

The Results pane is the middle pane. It has two sections, a Results grid and a Details window.

The results grid has the following information:

- Name the name of the Certificate object. This field is blank if the Plugin finds a certificate from a Network scan that isn't currently in the Policy Tree.
- Issued Shows when the certificate was issued. Demonstrates that the certificate has been issued after the date of the vulnerability.
- Subject Subject DN of the discovered certificate.
- CA the associated Certificate Authority. Will be blank if the Certificate is not in the Policy Tree or if the certificate is not associated to a Certificate Authority.
- Owner –Name of the contact/owner for the certificate.
- Details If a network scan detected a security problem, the most important issue is listed. Otherwise it will list the IP:port that where the certificate was found.

Results					
Name	Issued	Subject	CA	Owner	Detail
cachacarianacional.com.br	1/16/2013 12:0	CN=cachacar	Internal SSL (1-Year SHA256)	Admin	
mail.septier.com	4/21/2013 8:37:	CN=mail.sept	Internal SSL (1-Year SHA256)	Admin	
netaess2.netacom.com	3/31/2012 6:11:	CN=netaess2	Internal SSL (1-Year SHA256)	Admin	
web-stage-1.uarts.edu	2/23/2010 8:18:	CN=web-sta	Internal SSL (1-Year SHA256)	Admin	
FL10VM000000000	10/11/2011 9:2	E=support@	Internal SSL (1-Year SHA256)	Admin	
www.321rockets.com	1/22/2013 3:08:	CN=www.32	Internal SSL (1-Year SHA256)	Admin	

When an individual certificate is selected from the results grid, its details are populated in the Details window. The following information is available in the Details window:

- Distinguished Name the full path of the certificate in the Policy Tree
- Certificate Authority the CA template name and type of certificate authority object linked to the certificate
- Details If a network scan detected a security problem, the most important issue is listed here. Otherwise it will list the IP:port where the certificate was found.
- Status Current processing status of the certificate
- Owner Name of the current contact/owner of the certificate
- Disabled Whether the certificate object is currently disabled
- Certificate the full Subject DN (Distinguished Name) of the certificate
- Associated Applications Total number of applications associated to the certificate

Details	
Distinguished Name:	\VED\Policy\Certificates\Lab 09 - Workflows\Lab09 Certificate
Certificate Authority:	Internal SSL (1-Year SHA256) [Microsoft]
Detail:	
Status:	Ok
Owners:	99Alice
Disabled:	Yes
Certificate:	CN=*.lab.venafi.com, OU=Education Services, O=Venafi, L=Salt Lake City, S=Utah, C=
Associated Applications:	2 applications

If you click on the "Certificate:" link then you will see a pop-up window with the full certificate details:

Certificate Details	×
Path	
⊡	A 1
Details	
Field	Value
Subject	CN=*.lab.venafi.com, OU=Education Services, O=Venafi, L=Salt Lake City, S=Utah, C=US
Issuer	CN=traininglab-Root-CA, DC=traininglab, DC=local
Valid From	6/4/2013 5:42:29 AM
Valid To	6/4/2015 5:42:29 AM
Serial	66D2A6680000000009C
Signature	sha1RSA
Subject Key Identifier	bf 13 b9 f6 c9 b1 bc e0 c7 e3 df db 30 10 62 71 d2 01 22 36
Authority Key Identifier	KeyID=70 a8 d6 62 19 ad bd 7e a0 bc d7 06 47 c6 75 6d 97 05 eb 0d
CRL Distribution Points	[1]CRL Distribution Point: Distribution Point Name:Full Name:URL=Idap:///CN=traininglab-Root-CA,CN=server1,CI
Authority Information Access	[1]Authority Info Access: Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2), Alternative
Certificate Template Name	WebServer
Key Usage	Digital Signature, Key Encipherment (a0)
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)

If you click on the "Associated Applications:" link you will see a list of the Associated Applications and their corresponding status:



IMPORTING RESULTS INTO POLICY TREE FROM NETWORK SCAN

Certificate results cannot be added to the Work Queue unless the certificate exists in the policy tree. New certificates that are found during a network scan can be imported into the Policy Tree so that the certificates can be protected.

Results								
Name	Issued	Subject 🔺	CA	Owner	Detail			
	9/7/2013 12:00:00 AM	CN=*.my.yahoo.com, O=Yahoo! Inc., L			Weak hashing algorithm (sha1RSA) found at 98.138.250.118:			
	6/24/2013 12:00:00 AM	CN=*.playerio.com, OU=PositiveSSL Wi			Weak hashing algorithm (sha1RSA) found at 98.138.219.138:			
	4/1/2013 12:00:00 AM	CN=*.secure.webhosting.yahoo.com,			Weak hashing algorithm (sha1RSA) found at 98.138.222.94:443			
	9/30/2013 12:00:00 AM	CN=*.thumb.mail.yahoo.com, O=Yaho			Heartbleed vulnerability found at 98.138.214.104:443			
	6/5/2013 12:00:00 AM	CN=*.voices.yahoo.com, O=Yahoo! Inc			Weak hashing algorithm (sha1RSA) found at 98.138.250.195:			
	2/20/2014 9:34:41 AM	CN=*.yahoo.com, OU=APG, O=Yahoo!,			Weak key strength (1024 bits) found at 98.138.231.164:443			
	6/13/2012 6:46:16 AM	CN=*.yahoo.com, OU=CMP, O=Yahoo!			Weak key strength (1024 bits) found at 98.138.231.240:443			
	3/16/2012 6:27:08 AM	CN=*.yahoo.com, OU=TnS, O=Yahoo,			Weak key strength (1024 bits) found at 98.138.231.162:443			
	4/8/2014 12:00:00 AM	CN=*.yimg.com, OU=Information Tech			Weak hashing algorithm (sha1RSA) found at 98.138.219.13:443			
	1/23/2012 10:57:42 AM	CN=api.int1.yieldmanager.com, OU=Ya			Weak hashing algorithm (md5RSA) found at 98.138.231.86:443			

- 1. Select a certificate from the Results grid
- 2. Click the "Import" button
- 3. Select the Owner, Policy, and Certificate Authority template and click "Create"

🗟 Import Certificates	
The certificate(s) will be location of your choice. for it, with the selected configured with the cer	e imported into a policy named 'Bulk Import' in a A device and basic application will be created owner assigned, and the policy will be tificate template you select.
Owner:	LDAP+Lab:Aaron Hixson
Create under Policy:	\VED\Policy\Certificates
Certificate Authority:	\VED\Policy\Administrator\Certificate
	<u>C</u> ancel C <u>r</u> eate

Note: the certificates will be created in a "Batch Import" policy within the policy you selected.

4. The results column will update with the new object name from the policy tree.

Results										
Name	Issued	Subject	CA	Owner	Detail 🔺					
.thumb.mail.yahoo	9/30/2013 12:00:00 AM	CN=.thumb.mail.yahoo.com, O=Yaho	Internal SSL (1-Ye		Heartbleed vulnerability found at 98.138.214.104:443					
	8/8/2013 12:00:00 AM	CN=*.attach.mail.ymail.com, O=Yahoo!			Weak hashing algorithm (sha1RSA) found at 98.138.215.41:443					
	11/20/2013 12:00:00 AM	CN=*.attach.mail.yahoo.com, O=Yahoo			Weak hashing algorithm (sha1RSA) found at 98.138.215.63:443					

ADDING RESULTS TO THE WORK QUEUE

As you review results from various search types, you can select certificates individually or in groups to be added to the Work Queue. You can use CTRL + A to select all results from the Results grid.

Things to check for before adding to the Work Queue

Certificates in certain circumstances can get you into to trouble. Be sure to check your certificates before you add them to the Work Queue for bulk revocation/renewing

- Make sure the certificate is enabled
- Make sure the certificate is set to enrollment or provisioning
- Make sure the certificate has an associated Certificate Authority if you plan to revoke
- Make sure the certificate is not currently processing or in an error state
- Make sure your policies are configured so that TrustAuthority generates the private key and CSR
- If the Certificate Authority has required vendor specific fields, make sure the fields are completed via policy.

After you feel comfortable with the certificates in your results grid, select the certificates and click "Select" to add them to the Work Queue in the third (left) panel.

THE WORK QUEUE

REVIEWING QUEUE DETAILS

Unlike the Results panel, the Work Queue panel is persistent and attempts to auto save your progress as you build your work queue. If you need to exit the Venafi Vulnerability Remediation Plugin, it is recommended that you save the queue so that you do not lose your work. Work queues can be cleared, saved, and loaded from the File menu.

🛃 Bul	🚳 Bulk Certificate Management								
File	Reports								
	Clear Queue	Ctrl+N							
12	Load Queue	Ctrl+O							
	Save Queue	CtrI+S							
	Exit								

REMOVING CERTIFICATES FROM THE QUEUE

If you decide you'd like to remove selected certificates from the Work Queue in the third (left) panel, you can highlight those certificates and click the "Remove" button.

Remove

STARTING WORK

After you feel comfortable with the current Work Queue, click the "Start Work" button.



When you click "Start Work" the "Select Work Type" dialog appears asking what type of work you'd like to do:

- Renew queued certificates This will renew each certificate in the Work Queue list with its respective Certificate Authorities
 Note: Certificates using the VeriSign VICE 2 certificate will automatically be renewed using the "Replace" enrollment mode.
- Revoke and renew queued certificates First revokes each certificate and then renews it with its respective Certificate Authority.
- Switch certificates to a different certificate authority Changes the configured CA template for all queued certificate and renews them via the new CA template object.

Select Work Type
Please choose one of the following workflows:
Renew queued certificates
Renews each queued certificate with its respective CA.
 Revoke and renew queued certificates
First revokes each certificate and then renews it with its respective CA.
Revocation reason: Certificate Superseded -
 Switch certificates to a different certificate authority (CA)
Changes the configured CA for all queued certificates and renews them via the new CA.
New CA:
Cancel Perform Work

Click the "Perform Work" can you have completed your selection on the "Select Work Type" dialog. Clicking "Perform Work" will immediately queue up all renewals and revocations (if applicable) in bulk.

THE PROCESSING WINDOW

Bulk Lertificate Management										
Queue		Revoked				Renewed				
Name Subject CA Owner	Nar	me	Subject	CA	Owner	Name	Issued	Subject	CA	
mobile.navyfed CN=mobile.nav Internal SSL (1 Admin	-									
www.ncmlinke CN=www.ncml Internal SSL (1 Admin										
Wildcard.meth CN=*.methodh Internal SSL (1 Admin										
www.10bis.co.il CN=www.10bi Internal SSL (1 Admin										
www.kpmginst CN=www.kpm Internal SSL (1 Admin										
kmamr-ext.acce CN=kmamr-ext Internal SSL (1 Admin										
FGT60D461300 E=support@fo Internal SSL (1 Admin										
audit.us.kpmg CN=audit.us.k Internal SSL (1 Admin										
www.costproje CN=www.cost Internal SSL (1 Admin										
alliances.accen CN=alliances.a Internal SSL (1 Admin										
ikwyat.com E=root@ikwyat Internal SSL (1 Admin										
hcsc.equasiis.net CN=hcsc.equas Internal SSL (1 Admin										
personalsaving CN=personalsa Internal SSL (1 Admin										
www.semitwist E=semitwist@ Internal SSL (1 Admin										
www.cool.army CN=www.cool Internal SSL (1 Admin										
ucb.equasiis.net CN=ucb.equasi Internal SSL (1 Admin										
vpn-dr.dexia-is CN=vpn-dr.dex Internal SSL (1 Admin										
SAPPC2.ACCEN CN=SAPPC2.AC Internal SSL (1 Admin										
www.mychartc CN=www.mych Internal SSL (1 Admin	-1									
crevents accent CN= crevents a Internal SSI (1. Admin									I	
827 certificate queued	0 0	ertificate revoke	d			0 certificate queue	d	🗐 Report.	. 🚺 Close	
Details		Details				Details				
Distinguished Name: \VED\Policy\Lab 11 - Secure _Protect\Resources\Inter	ne	Distinguished N	lame:			Distinguished I	Name:			
Certificate Authority: Internal SSL (1-Year SHA256) [Microsoft]		Certificate Authority:					Certificate Authority:			
Stage:		-	itage:				Stage:			
Status: Ok		S	tatus:				itatus:			
Owners: Admin		Ov	/ners:			0	vners:			
Certificate: CN=mobile.navyfederal.org, OU=Telecommunication	ns,	Certi	icate:			Certi	ficate:			
Associated Applications: 4 applications	Ass	sociated Applica	itions:			Associated Applic	ations:			
						1		ĺ		

INTRODUCTION

After the bulk work begins, the three windows are replaced with a new view called the processing window. This view shows you the progress of your certificates as they are revoked (if applicable) and renewed. The screen automatically refreshes as certificate work is done.

On this screen, you have the ability to click on the "Certificates" and "Associated Application" link to see further details for a highlighted certificate (similar to the information on the Results and Work Queue screen).

QUEUE

The queue pane on the left shows the work that needs to be done.

REVOKED

Certificates will show up in the Revoked pane after they have successfully been revoked and are waiting on being renewed

o Queue				Nevoked					
Name	Subject	CA	Owner		Name	Subject	CA	Owner	
mail.septier.com	CN=mail.septie	Internal SSL (1	Admin		timetable.netvi	CN=timetable	Internal SSL (1	Admin	
self-signed - 77	CN=self-signe	Internal SSL (1	Admin		www.proctorsil	CN=www.proc	Internal SSL (1	Admin	
www.mslinkeu	CN=www.msli	Internal SSL (1	Admin		rms.013netvisio	CN=rms.013net	Internal SSL (1	Admin	
webcastfms2.a	CN=webcastfm	Internal SSL (1	Admin		dbr1.timemake	CN=dbr1.time	Internal SSL (1	Admin	
www.polycom	CN=www.poly	Internal SSL (1	Admin		pob.hadassah	CN=pob.hadas	Internal SSL (1	Admin	
sslras2.us.kpm	CN=ssIras2.us	Internal SSL (1	Admin		Wildcard.pcch	CN=*.pcchu.ca,	Internal SSL (1	Admin	
.zappos.com	CN=.zappos.c	Internal SSL (1	01Admin		editingcareers3	CN=editingcar	Internal SSL (1	Admin	
tax.accenture.c	CN="tax.accent	Internal SSL (1	Admin		Sites	CN=Sites, O="	Internal SSL (1	Admin	
feeds.coffeegia	CN=feeds.coff	Internal SSL (1	Admin		www.srlinkes.k	CN=www.srlin	Internal SSL (1	Admin	
mail.opglaw.com	CN=mail.opgla	Internal SSL (1	Admin		*.medhokapps	CN=*.medhoka	Internal SSL (1	01Admin	
securepayment	CN=securepay	Internal SSL (1	Admin		www.greennur	CN=www.gree	Internal SSL (1	Admin	
www.bicestervi	CN=www.bices	Internal SSL (1	Admin		www.lflinke.kp	CN=www.lflink	Internal SSL (1	Admin	
www.fitnessso	CN=www.fitne	Internal SSL (1	Admin		msvcs_prod_ssl	CN=msvcs_pro	Internal SSL (1	Admin	
ltcfisocsae.fisgl	CN=ltcfisocsae	Internal SSL (1	Admin		secure.semclix	CN=secure.sem	Internal SSL (1	Admin	
socr.wrdsb.on.ca	CN=socr.wrdsb	Internal SSL (1	Admin		www.mvwlinke	CN=www.mvwl	Internal SSL (1	Admin	
citrix.aggwest.c	CN=citrix.aggw	Internal SSL (1	Admin		www.olsale.co.il	CN=www.olsal	Internal SSL (1	Admin	
timunix.cegep	CN=timunix.ce	Internal SSL (1	Admin		www.mvwlinke	CN=www.mvwl	Internal SSL (1	Admin	
www.nevikor.c	CN=www.nevi	Internal SSL (1	Admin		home2.iba.org.il	CN=home2.iba	Internal SSL (1	Admin	
Wildcard.cosm	CN=*.cosmeo.c	Internal SSL (1	Admin		topup.cctwirel	CN=topup.cct	Internal SSL (1	Admin	
chootswebacce	CN=chcctsweb	Internal SSL (1-	Admin	_ _ _	insistal moves	CN=nsssta1 ms	Internal SSI (1-	Admin	

RENEWED

Certificates will show up in the Renewed pane after renewal is complete and all processing has been done.

Note: the "Done" button has an approximate 30-second delay after all work is complete before it can be selected.

🗟 Bulk Certificate Management													
File Reports													
Queue					Revoked					Renewed	l		
Name	Subject	CA	Owner		Name	Subject	CA	Owner .	1	Name	Issued	Subject	CA
www.asa.net	CN=www.asa	Internal SSL (1	Admin		timetable.netvi	CN=timetable	Internal SSL (1	Admin		self-signed - 77	4/15/2014 2:43:	CN=self-signe	Internal SSL (1
webclient.bank	CN=webclient	Internal SSL (1	Admin		www.proctorsil	CN=www.proc	Internal SSL (1	Admin		FL10VM000000	4/15/2014 2:44:	CN=FL10VM00	Internal SSL (1
dashboard.fnt	CN=dashboard	Internal SSL (1	Admin		rms.013netvisio	CN=rms.013net	Internal SSL (1	Admin		www.votedou	4/15/2014 2:44:	CN=vvvv.vote	Internal SSL (1
rapideyetechn	CN=rapideyete	Internal SSL (1	Admin		dbr1.timemake	CN=dbr1.time	Internal SSL (1	Admin		tools.accenture	4/15/2014 2:44:	CN=tools.acce	Internal SSL (1
qa.en.pampers	CN=qa.en.pam	Internal SSL (1	01Admin		pob.hadassah	CN=pob.hadas	Internal SSL (1	Admin		eme.us.kpmg.c	4/15/2014 2:44:	CN=eme.us.kp	Internal SSL (1
xai-medica.com	CN=×ai-medica	Internal SSL (1	Admin		Wildcard.pcch	CN=*.pcchu.ca,	Internal SSL (1	Admin		bgt.oro.doe.gov	4/15/2014 2:44:	CN=bgt.oro.do	Internal SSL (1
www.travelerb	CN=www.trave	Internal SSL (1	Admin		editingcareers3	CN=editingcar	Internal SSL (1	Admin		www.alamodas	4/15/2014 2:44:	CN=www.alam	Internal SSL (1
www.kitsuji.com	CN=www.kitsu	Internal SSL (1	Admin		Sites	CN=Sites, O="	Internal SSL (1	Admin					
scm.accenture	CN=scm.accent	Internal SSL (1	Admin		www.srlinkes.k	CN=www.srlin	Internal SSL (1	Admin					
www.sglinkes	CN=www.sglin	Internal SSL (1	Admin		*.medhokapps	CN=*.medhoka	Internal SSL (1	01Admin					
ConnectingToo	CN=Connectin	Internal SSL (1	Admin		www.greennur	CN=www.gree	Internal SSL (1	Admin					
firmwide.us.kp	CN=firmwide.u	Internal SSL (1	Admin		www.lflinke.kp	CN=www.lflink	Internal SSL (1	Admin					
pm.cyberitas.com	CN=pm.cyberit	Internal SSL (1	Admin		msvcs_prod_ssl	CN=msvcs_pro	Internal SSL (1	Admin					
investall.kpmg	CN=investall.k	Internal SSL (1	Admin		secure.semclix	CN=secure.sem	Internal SSL (1	Admin					
piloq.cvm.qc.ca	CN=piloq.cvm	Internal SSL (1	Admin		www.mvwlinke	CN=www.mvwl	Internal SSL (1	Admin					
www.semitwist	CN=www.semi	Internal SSL (1	Admin		www.olsale.co.il	CN=www.olsal	Internal SSL (1	Admin					
emp.navyfeder	CN=emp.navyf	Internal SSL (1	Admin		www.mvwlinke	CN=www.mvwl	Internal SSL (1	Admin					
TCAM	CN=TCAM, OU	Internal SSL (1	Admin		home2.iba.org.il	CN=home2.iba	Internal SSL (1	Admin					
iplanet.emet.co.il	CN=iplanet.em	Internal SSL (1	Admin		topup.cctwirel	CN=topup.cct	Internal SSL (1	Admin					
hasrms accentu ∢	CN=hasrms acc	Internal SSI (1-	Admin	· [nssstri1 msves	CN=nssstri1 ms	Internal SSI (1-	Admin	-	•			•
152 certificate que	tificate queued 653 certificate revoked							7 certificate renew	ed	Report	Close		

REPORTS

WORK REPORT

After work is done an all certificates appear in the 'Renewed panel, the 'Report' button becomes available. Selecting 'Report' will generate a CSV file of all work that was performed.

Items included in the report:

- Full path in the policy tree of the certificate object
- Timestamp for revocation (if applicable)
- Timestamp for certificate renewal
- Name of new Certificate Authority template (if applicable)
- Certificate DN
- Certificate start validity timestamp
- Scan details (if applicable)

A	в	L	U	E	F	
Certificate DN	Revoked	Renewed	New CA	Certificate	Certificate Valid From	Detail
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\timetable.net	4/15/2014 14:53	4/15/2014 15:07		CN=timet	4/15/2014 14:57	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\www.proctors	4/15/2014 14:53	4/15/2014 15:09		CN=www.	4/15/2014 14:53	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\rms.013netvis	4/15/2014 14:53	4/15/2014 14:56		CN=rms.0	4/15/2014 14:43	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\dbr1.timemak	4/15/2014 14:53	4/15/2014 15:12		CN=dbr1.t	4/15/2014 15:01	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\pob.hadassah	4/15/2014 14:53	4/15/2014 15:00		CN=pob.h	4/15/2014 14:50	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\Wildcard.pcch	4/15/2014 14:53	4/15/2014 15:14		CN=*.pcch	4/15/2014 15:04	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\editingcareer	4/15/2014 14:53	4/15/2014 15:08		CN=editin	4/15/2014 14:45	
\VED\Policy\Lab 11 - Secure & Protect\Resources\Internet Scan\Sites	4/15/2014 14:53	4/15/2014 15:13		CN=Sites,	4/15/2014 14:59	
1		- * *				



After a network scan is performed, the results of the scan from the middle Results panel can be exported to a Scan report so that if vulnerabilities require patching any server software (eg. Heartbleed) than you can address those issues with the report before continuing with the key rotation and certificate renewal.

Items included in the report:

- Severity What is the severity of the vulnerability that was detected by the scan
- Host IP address of certificate find
- Port Listening port of certificate found
- Issue Lists the vulnerability found (Heartbleed, SHA1/MD5, Key length)

Severity	Host	Port	Issue	Certificate Subject
Critical	10.10.11.5	443	Heartbleed vulnerability found a	C=US, S=New York, L=New York, O=A Fine
Important	10.10.10.4	443	Weak hashing algorithm (sha1RS	CN=*.zappos.com, OU=Systems Administr
Important	10.10.10.2	443	Weak hashing algorithm (sha1RS	CN=qa.en.pampersrewards.pampers.com
Important	10.10.15.1	443	Weak hashing algorithm (sha1RS	CN=*.medhokapps.com, OU=Domain Cont
Important	10.10.17.4	443	Weak hashing algorithm (sha1RS	CN=SUBWAY, OU=EDI, O=IT, L=MILFORD, S

TROUBLESHOOTING

Certificate processing typically runs into problems when the certificate is in a state where it can't be renewed, such as:

- Wrong management type
- Missing required fields (CA Template or Vendor specific required fields)
- Certificate was already in error

Workflow

Workflows still need to be approved for when bulk renewals and revocations are performed. These are not bypassed by the Plugin.

Source File

There is a file called WinAdminBulkCertSelected.txt stored in %AppData%\Venafi, Inc\Venafi Encryption Director\{Version}\. This file is what keeps track of the work currently being done and attempts to automatically save progress in case the Plugin is closed.

Certificates Stuck in Processing

Certificates will stay in the "Queued" window if they encounter errors during revocation or renewal. Clicking on individual certificates will show the stage and status of the certificate in the detail window. Login to Web Admin to address the issue for each certificate. The Processing Window will automatically refresh as certificates continue to process. If fixing the issues are not available, close the Plugin and move the Plugin source file to a new location.

Known Issue

- Scanned certificates will always show that they are being Monitored, even if they do not exist in the Policy Tree
- Using the feature "Scan Existing Devices" will not work if any device objects in the policy tree have the hostname of "localhost"

LOGGING

When the Venafi Vulnerability Remediation Plugin is used, much of the same logging from automated renewals that happens in the platform is still logged. The primary items that are not currently logged by the Plugin are the action items that the Plugin automates like the clicking of "Revoke" or "Renew Now". The logs continue to be extremely valuable for troubleshooting purposes.