

RSA

RSA[®] ARCHER[®] SUITE
Integration Guide

Tenable.sc[™] Data Feeds for RSA Archer

IT Security Vulnerability Program 6.7



Contact information

Go to the RSA corporate website for regional Customer Support telephone and fax numbers:<https://community.rsa.com/community/rsa-customer-support>.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and Dell are either registered trademarks or trademarks of Dell Corporation ("Dell") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on RSA.com. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

For secure sites, Dell recommends that the software be installed onto encrypted storage for secure operations.

For customers in high security zones, Dell recommends that a full application sanitization and reinstallation from backup occur when sensitive or classified information is spilled.

Note on Section 508 Compliance

The RSA Archer® Suite is built on web technologies which can be used with assistive technologies, such as screen readers, magnifiers, and contrast tools. While these tools are not yet fully supported, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for RSA Archer.

The RSA Archer Mobile App can be used with assistive technologies built into iOS. While there remain some gaps in support, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for the RSA Archer Mobile App.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. Use of the software described herein does not ensure compliance with any laws, rules, or regulations, including privacy laws that apply to RSA's customer's businesses. Use of this software should not be a substitute for consultation with professional advisors, including legal advisors. No contractual obligations are formed by publication of these documents.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright 2010-2020 Dell, Inc. or its subsidiaries. All Rights Reserved.
August 2020

Table of Contents

Release 6.7	4
Chapter 1: Overview	4
Summary	4
Key Features and Benefits	4
Requirements.....	4
Integration Diagram	5
Chapter 2: Configurations.....	6
System Requirements	6
Data Feed Configuration.....	7
Data Feeds	7
Configure the JavaScript Transporter Settings	9
Digital Thumbprints.....	9
RSA Security LLC Cert in the Trusted Root CA Store.....	9
Obtaining a Certificate Thumbprint.....	10
Set Up the Tenable.sc Plugins RSA Archer 6.7 Data Feed.....	11
Set Up the Tenable.sc Hosts RSA Archer 6.7 Data Feed.....	15
Set Up the Tenable.sc Vulnerabilities Archer 6.7 Data Feed.....	20
Chapter 3: Using the Tenable.sc Data Feeds	26
Scheduling Data Feeds.....	26
Appendix A: Certification Environment.....	28

Release 6.7

Chapter 1: Overview

Summary

Tenable.sc™ consolidates and evaluates vulnerability data across your organization, while prioritizing security risks and providing a clear view of your security posture. Built on Nessus technology, Tenable.sc discovers unknown assets that can be cataloged as part of your asset inventory.

The integration of Tenable.sc with the RSA Archer IT & Security Vulnerabilities Program use case enables customers to leverage the discovered devices and catalog those network devices with the vulnerability library. With RSA Archer, customers can then identify which assets require remediation based on the business priority of that asset.

Key Features and Benefits

The Tenable.sc integration with RSA Archer enables organizations to do the following:

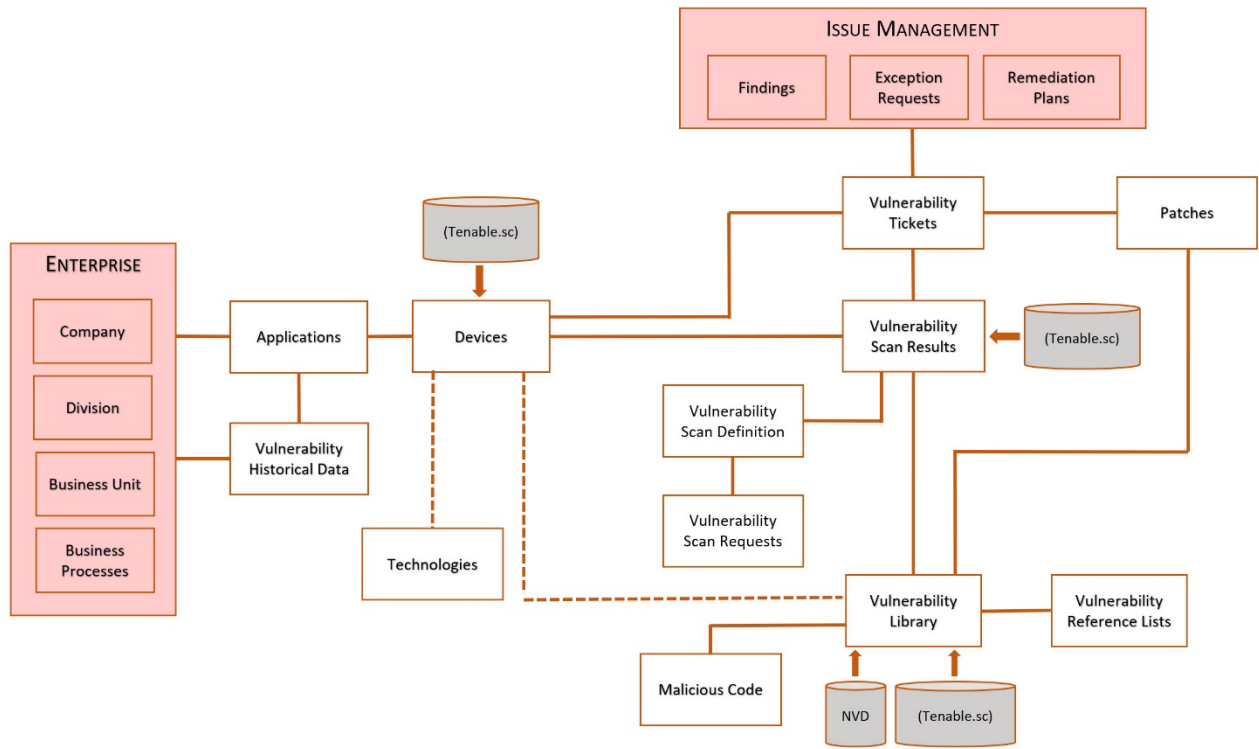
- Supplement the Vulnerability Library application with plugin content, which includes extensive CVE coverage.
- Discover and catalog of assets, including unauthorized assets.
- Capture network vulnerabilities using scanning technologies.
- Gain quick visibility to assess risk posture on critical infrastructure devices.
- Validate vulnerabilities inside RSA Archer once scanners no longer detect vulnerabilities.

Additionally, Tenable.sc calculates a Vulnerability Priority Rating score, which is a combination of the threat intelligence and machine learning to determine the likelihood a vulnerability will be exploited inside your environment.

Requirements

Components	Requirement
RSA Archer Solution	IT & Security Risk Management
RSA Archer Use Case	IT Security Vulnerabilities Program
RSA Archer Applications	Devices, Vulnerability Library, and Vulnerability Scan Results
Requires On-Demand License	No

Integration Diagram



Chapter 2: Configurations

This section provides instructions for configuring the Tenable.sc data feeds with the RSA Archer Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Tenable.sc components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Important: The RSA Archer IT Security Vulnerabilities Program use case and the Enterprise Catalog package must be installed and working prior to performing the integration. Perform the necessary tests to confirm that this is true prior to proceeding.

Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

System Requirements

The following components are required for installation and operation of the Tenable.sc data feeds for the IT Security Vulnerabilities Program use case. The applications listed in the following table serve as the targets for the data feeds.

Component	Details
RSA Archer	RSA Archer 6.7
Prerequisite Applications (RSA Archer IT Security Vulnerabilities Program)	<ul style="list-style-type: none">• Devices• Vulnerability Library• Vulnerability Scan Results

Data Feed Configuration

Data Feeds

Tenable.sc provides a REST API that allows for the capability to script in interactions directly with the Tenable.sc server. With RSA Archer JavaScript Transporter our clients can easily authenticate to the server and make multiple, dependent API calls extracting large amounts of data in a single data feed.

The following data feeds are provided with this integration:

Data Feed	Description
Tenable.sc Plugins RSA Archer 6.7	The Tenable.sc Plugins RSA Archer 6.7 feed is a JavaScript Transporter feed that utilizes API calls to extract all requested plugin definitions. Tenable.sc data is imported and leveraged in the Vulnerability Library application.
Tenable.sc Hosts RSA Archer 6.7	<p>The Tenable.sc Hosts RSA Archer 6.7 feed is a JavaScript Transporter feed that utilizes API calls to extract all the asset inventory discovered based on a client's scanner configuration and implementation. Tenable.sc data is imported and leveraged in the Devices application.</p> <p>For data ingestion, RSA Archer offers configurable settings that allow individual clients to define how to uniquely identify devices in their organization.</p>
Tenable.sc Vulnerabilities RSA Archer 6.7	<p>The Tenable.sc Vulnerabilities RSA Archer 6.7 feed is a JavaScript Transporter feed that utilizes API calls to extract the vulnerabilities detected on each asset.</p> <p>For data ingestion, RSA Archer offers configurable settings that allow individual clients to define how to uniquely identify devices in their organization. However, it is critical to note that any alteration of the unique identifier for this feed must continue to include the Repository ID as defined by Tenable.sc.</p>

Important: You must install all package files before importing data feeds. Package files include the IT Security Vulnerabilities Program use case package, the Enterprise Catalog package, and the Issues Management prerequisite use case package. For more information, see the "Installing the Packages" section of the IT Security Vulnerabilities Program use case in the RSA Archer Online Documentation.

Import and run the data feeds in the following order:

- (Optional) NVD Data Feeds
Note: For information on setting up the NVD data feeds, see the *NIST National Vulnerability Database (NVD) Data Feeds for RSA Archer IT Security Vulnerability Program Implementation Guide* on the RSA Exchange on RSA Link.
- Tenable.sc_Plugins_RSA_Archer_6.7.dfx5
- Tenable.sc_Hosts_RSA_Archer_6.7.dfx5

4. Tenable.sc_Vulnerabilities_RSA_Archer_6.7.dfx5

Note: After setting up the data feeds, you can schedule the feeds to run when you want to. For more information, see the Scheduling Data Feeds section.

Note: Tenable.sc documentation and the API best practice guide can be found on its website (<https://docs.tenable.com/Tenable.sc.htm>).

Configure the JavaScript Transporter Settings

Before you upload a JavaScript file, you must configure JavaScript Transporter settings in the RSA Archer Control Panel.

1. On the General tab, go to the JavaScript Transporter section.
 1. Open the RSA Archer Control Panel.
 2. Go to Instance Management and select All Instances.
 3. Select the instance.
 4. On the General tab, go to the JavaScript Transporter section.
2. Set the Max Memory Limit and the Script Timeout variable to align with the resources necessary to retrieve data. Most incremental feeds can probably be achieved with a Max Memory Limit of 3048 MB (3 GB) and a Script Timeout of 300 minutes (5 hours).
3. Require Signature is enabled by default on install and required for all Hosted clients.
 - a. In the Signing Certificate Thumbprints section, add a thumbprint for each digitally signed JavaScript file.
 - i. Double-click an empty cell in the Signing Certificate Thumbprints section.
 - ii. Enter the digital thumbprint of the trusted certificate used to sign the JavaScript file.

Note: For information on how to obtain digital thumbprints, see [Obtaining Digital Thumbprints](#).

Important: If you enable Require Signature and do not specify thumbprints, JavaScript files will not be accepted by the system.
4. On the toolbar, click Save.

Digital Thumbprints

When running JavaScript data feeds, you can set the system to only allow digitally signed JavaScript files from trusted sources for security considerations.

For a certificate to be trusted, all the certificates in the chain including the Root CA Certificate and Intermediate CA certificates must be trusted on both the Web Server and Services Server machines.

RSA Security LLC cert in the Trusted Root CA Store

RSA Security LLC certificate is not present on every machine's root by default.

1. On the JavaScript file, Right-click and select Properties.
 - a. Click the Digital Signatures tab.
 - b. From the Signature List window, select RSA Security LLC.
 - c. Click the Details button
 - d. Click View Certificate.

- e. Click Install Certificate.
 - f. Select Local Machine, and click Next.
 - g. Select Place all certificates in the following store, and click Browse.
 - i. Select Trusted Root Certification Authorities, and click OK.
 - ii. Click Next.
 - iii. Click Finish.
2. Upon successful import, click OK.

Obtaining a Certificate Thumbprint

1. On the Web Server and Services Server machines, open the Manage Computer Certificates program.
 - a. Launch “certmgr” from the Start menu.
 - b. Navigate to Certificates – Local Computer > Trusted Root Certification Authorities > Certificates.
 - c. Ensure the following certificates are located in the Certificates sub-folder of the Trust Root Certification Authorities folder.
 - i. RSA Security LLC
 - ii. RSA Security 2048 V3 (Standard certificate)
2. Verify that the certificate is trusted.
 - a. Double click the RSA Security LLC certificate.
 - b. In the Certificate window, click the Certification Path tab.
 - c. Ensure that the Certificate Status windows displays the following message: “This certificate is OK”.

Note: If the Certificate Status windows displays something different, follow the on-screen instructions.

3. Obtain the trusted certificate thumbprint.
 - a. In the Certificate window, click the Details tab.
 - b. Scroll to, and select, the Thumbprint field.
 - c. The certificate's digital thumbprint appears in the window. Copy thumbprint.


Note: For information on adding digital thumbprints, see Step 4a of “Configure the JavaScript Transporter Settings” section of the document, regarding where thumbprint is relevant.

Set Up the Tenable.sc Plugins RSA Archer 6.7 Data Feed

Important Migration Note: If you have an existing integration, you must make some adjustments to your existing data due to the rebranding of Security Center to Tenable.sc. In the existing Vulnerability Library data for all existing Security Center data, change the **DFM Key** from "Security Center-ID" to "Tenable.sc-ID". Depending on your current integrations into this application, it might be as simple as turning the **DFM Key** into a calculated field. Example: `CONCATENATE([Source], "-", [ID])`

Important: Before you upload a JavaScript file, configure JavaScript Transporter settings in the RSA Archer Control Panel. For more information, see [Configure the JavaScript Transporter Settings](#).

Important: With the exception of the optional parameters specified in this procedure, changes to the JavaScript Transporter configuration file can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

1. Go to the Manage Data Feeds page.
 - a. From the menu bar, click .
 - b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the Tenable.sc_Plugins_RSA_Archer_6.7.dfx5 file.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. In the Additional Properties section, enable Optimize Calculations.
7. Click the Transport tab.
8. In the Transport Configuration section, complete the following:
 - a. Click Upload.
 - b. From the Upload JavaScript File dialog, click Add New.
 - c. Locate and select the Signed-TenableSC_v1_0_13.js file, and click Open.
 - d. From the Upload JavaScript File dialog, click OK.
9. The JavaScript code allows clients to pass in different variables through our Custom Parameters section. The following table describes the supported values for specific Custom Parameters.

Key	Value	Description
dataSource	Only one valid value	
	Default = vulns	
url	Requires valid value	
	Default = [empty]	

Tenable.sc Data Feeds for RSA Archer ITSVP 6.7

username	Requires valid value Default = [empty]	
password	Requires valid value Default = [empty]	
proxy	Optional Default = [empty]	
ignoreLastRunTime	Requires valid value Default = false	<p>LastRunTime is a token supplied in the data feed, and by default is the date used in the query logic. In order to use startDate, the ignoreLastRunTime parameter must be set = true.</p> <p>Date Logic:</p> <ul style="list-style-type: none"> • If ignoreLastRunTime = false and LastRunTime token is empty <ul style="list-style-type: none"> ○ Default to 1970-01-10T00:00:00Z • If ignoreLastRunTime = false and LastRunTime token is not empty <ul style="list-style-type: none"> ○ Use the LastRunTime token • If ignoreLastRunTime = true and startDate is empty <ul style="list-style-type: none"> ○ Default to 1970-01-10T00:00:00Z • If ignoreLastRunTime = true and startDate is not empty <ul style="list-style-type: none"> ○ Use startDate parameter specified by client
startDate	Optional Default = [empty]	<p>Additional parameter that allows clients to apply minimal, built-in search filter criteria for data extraction.</p> <p>The plugin query retrieves all plugin data over a specified range by passing values to the startOffset and endOffset values in the query. The startOffset value always defaults to "0", while the endOffset is the last record in the range. By default, endOffset is a numerical value equal to the equivalent of the current date + 1. Below is an example of how the logic is applied (extraction of data is by batchSize = 1000):</p> <ul style="list-style-type: none"> • Run query where startOffset=0, endOffset=1000 <ul style="list-style-type: none"> ○ If the modifiedTime >= "<i>startDate</i>", write data to file • Run query startOffset=1000, endOffset=2000 <ul style="list-style-type: none"> ○ If the modifiedTime >= "<i>startDate</i>", write data to file

Tenable.sc Data Feeds for RSA Archer ITSVP 6.7

		<ul style="list-style-type: none"> Run query with startOffset=2000, endOffset=3000 <ul style="list-style-type: none"> If the modifiedTime >= "<i>startDate</i>", write data to file Repeat the process until no data is returned from the plugin query, indicating the last record has been reached.
verifyCerts	Default = false [Configurable value of true / false]	Validates the website address matches the address on the certificate, similar to browser level validation.

Important: The keys and values are case-sensitive and cannot include extra spaces at the end of the strings. The listed values are in place by default but can be configured to suit your environment.

Note: Tenable.sc treats startOffset as exclusive. And while the query sorts by "modifiedTime", it should be noted Tenable.sc automatically invokes a secondary ascending sort on plugin ID. This is relevant in the event the data return from Tenable is greater than the batchSize indicated. By the web call automatically applying the plugin ID ascending as the secondary sort, we are now assured the query will return all data in the same order on every execution, as "id" is unique to the plugin query.

10. The following additional parameters are valid options for the Custom Parameters section for the current JavaScript file.

Key	Value	Description
batchSize	Default = 1000 (records at a time) [Configurable]	Used for defining batches of content to be retrieved in a single call. JavaScript makes incremental calls to pull the next batch of data.
socketLimit	Default = 10 [Configurable value of 1-25]	Indicates the maximum number of open socket channels to an endpoint to be used for TCP connections.
maxRetry	Default = 1 [Configurable value of 0-2]	Indicates the amount of times a retry will occur where a "socket hung up" error is encountered. If a retry is unsuccessful and the maxRetry is exceeded, the data feed will fail.

Tenable.sc Data Feeds for RSA Archer ITSVP 6.7

requestsPerMin	Default = 60 [Configurable value]	A parameter to allow clients to govern the number of API requests made by RSA Archer to the external integration.
lastRunTimeOffset	Default = -1 [Configurable value]	Ensures no data loss in the scenarios where calculations with Datetime can be a factor.

11. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.
12. Click the Source Definition tab.
 - a. Click the Tokens sub-tab.
 - b. Verify token values.

The following table describes token values to verify.

Token	Value
LastRunTime	(Populated by feed)

Note: For more information about tokens, see "Data Feed Tokens" in the RSA Archer Online Documentation.

13. Verify that key field values are not missing from the data feed setup window.
14. Click Save.

Note: Temporal scores reflect characteristics of the vulnerability that change over time. Since temporal scores are optional, in the case where temporal scores are not provided, RSA Archer applies by default the metric value that has no effect on the overall CVSS score. Default values simulate 'skipping' the impacts where users feel a specific metric does not apply.


Set Up the Tenable.sc Hosts RSA Archer 6.7 Data Feed

For the acquiring asset inventory from the scanner data, we use the vulnTool = sumip in the query to make the web call to the API. IP Summary is a view of aggregated data through Analysis endpoint. Therefore, the aggregation of IPs is still a byproduct of the discovered vulnerabilities.

Important: Before you upload a JavaScript file, configure JavaScript Transporter settings in the RSA Archer Control Panel. For more information, see [Configure the JavaScript Transporter Settings](#).

Important: With the exception of the optional parameters specified in this procedure, changes to the JavaScript Transporter configuration file can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

Important: RSA Archer implements with a unique key on DNS identification. However, we understand that environment configurations are unique across the infrastructure of an organization, therefore the unique key to identify if a Device already exists inside RSA Archer, is configurable to each client. And where clients have multiple scanners scanning the same set of devices or IP ranges, the unique key should be altered to a matching algorithm that identifies the device, regardless of the source.

1. Go to the Manage Data Feeds page.
 - a. From the menu bar, click .
 - b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the Tenable.sc_Hosts_RSA_Archer_6.7.dfx5 file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. In the Additional Properties section, enable Optimize Calculations.
7. Click the Transport tab.
8. In the Transport Configuration section, complete the following:
 - a. Click Upload.
 - b. From the Upload JavaScript File dialog, click Add New.
 - c. Locate and select the Signed-TenableSC_v1_0_13.js file, and click Open.
 - d. From the Upload JavaScript File dialog, click OK.

9. The JavaScript code allows clients to pass in different variables through our Custom Parameters section. The following table describes the supported values for specific Custom Parameters.

Key	Value	Description
dataSource	Only one valid value Default = hosts	
url	Requires valid value Default = [empty]	
username	Requires valid value Default = [empty]	
password	Requires valid value Default = [empty]	
proxy	Optional Default = [empty]	
hostSeverities	Requires valid value Default = 4,3,2,1,0	Filter passed to the query. Eliminates unwanted host data from the query results. Data is only returned where the host were discovered on vulnerabilities with the defined severity levels. 4 = Critical; 3 = High; 2 = Medium; 1 = Low; 0 = Informational
vulnDateFilterType	Default = firstSeen [Configurable value, but only one value allowed]	Filter passed to the query. We calculate the concept of a startDate and endDate, by using either the LastRunTime token, startDate parameter, or a default date value. The selected date is then used as the filter logic passed as part of the query to eliminate unwanted hosts being returned. Example: "filters": { "filterName": "firstSeen", "operator": "=", "value": "#:#" } Valid filterName values: <ul style="list-style-type: none"> firstSeen - Equivalent to filtering on Vulnerability Discovered on the Vulnerability Analysis page of the Tenable.sc user interface. Both the

		<p>“vulnLoadActive” and “vulnLoadPatched” parameters can be used to limit the query results.</p> <ul style="list-style-type: none"> • lastSeen - Equivalent to filtering on Vulnerability Observed on the Vulnerability Analysis page of Tenable.sc user interface. This variable requires “vulnLoadPatched” = false. • lastMitigated – Equivalent to filtering on Vulnerability Mitigated on the Vulnerability Analysis page of Tenable.sc user interface. This variable requires “vulnLoadActive” = false. <p>Logic to calculate the value criteria:</p> <ul style="list-style-type: none"> • First value is always = 0. This represents a value of Today, or the last possible data point that can be returned from Tenable.sc. • The second value in the criteria is a numerical value represented by days prior to today.
ignoreLastRunTime	<p>Requires valid value</p> <p>Default = false</p>	<p>LastRunTime is a token supplied in the data feed, and by default is the date used in the query logic. In order to use startDate, the ignoreLastRunTime parameter must be set = true.</p> <p>Date Logic:</p> <ul style="list-style-type: none"> • If ignoreLastRunTime = false and LastRunTime token is empty <ul style="list-style-type: none"> ○ Default to 1970-01-10T00:00:00Z • If ignoreLastRunTime = false and LastRunTime token is not empty <ul style="list-style-type: none"> ○ Use the LastRunTime token • If ignoreLastRunTime = true and startDate is empty <ul style="list-style-type: none"> ○ Default to 1970-01-10T00:00:00Z • If ignoreLastRunTime = true and startDate is not empty <ul style="list-style-type: none"> ○ Use startDate parameter specified by client
startDate	<p>Optional</p> <p>Default = [empty]</p>	<p>Additional parameter, other than LastRunTime token, that allows clients to apply minimal, built-in search filter criteria for data extraction.</p> <p>An example of how the logic is applied (extraction of data is by batchSize = 1000, vulnDataFilterType = firstSeen, and startDate = 2019-04-21):</p> <ul style="list-style-type: none"> • Calculate the "value" criteria in firstSeen. <ul style="list-style-type: none"> ○ 0:370 (ie. 4/21 = 370 days ago)

		<ul style="list-style-type: none"> • Run query using filter criteria and where startOffset=0, endOffset=1000 <ul style="list-style-type: none"> ○ Write data to file • Run query using filter criteria and where startOffset=1000, endOffset=2000 <ul style="list-style-type: none"> ○ Write data to file • Repeat the process until no data is returned from the query, indicating the final value in firstSeen criteria has been reached.
vulnLoadActive	<p>Requires valid value</p> <p>Default = true</p> <p>[Configurable value of true or false]</p>	Indicates whether to pull data from the Cumulative database. Also known as the Active database.
vulnLoadPatched	<p>Requires valid value</p> <p>Default = true</p> <p>[Configurable value of true or false]</p>	Indicates whether to pull data from the Mitigated database. Also known as Patched database.
verifyCerts	<p>Default = false</p> <p>[Configurable value of true or false]</p>	Validates the website address matches the address on the certificate, similar to browser level validation.

Important: The keys and values are case-sensitive and cannot include extra spaces at the end of the strings. The listed values are in place by default but can be configured to suit your environment.

Note: Tenable.sc treats startOffset as exclusive.

10. (Optional) The following additional parameters are valid options for the Custom Parameters section for the current JavaScript file.

Key	Value	Description
batchSize	<p>Default = 1000 (records at a time)</p> <p>[Configurable]</p>	Used for defining batches of content to be retrieved in a single call. JavaScript makes incremental calls to pull the next batch of data.
socketLimit	<p>Default = 10</p> <p>[Configurable value of 1-25]</p>	Indicates the maximum number of open socket channels to an endpoint to be used for TCP connections.
maxRetry	<p>Default = 1</p>	Indicates the amount of times a retry will occur where a "socket hung up" error is

	[Configurable value of 0-2]	encountered. If a retry is unsuccessful and the maxRetry is exceeded, the data feed will fail.
requestsPerMin	Default = 60 [Configurable value]	A parameter to allow clients to govern the number of API requests made by RSA Archer to the external integration.
lastRunTimeOffset	Default = -1 [Configurable value]	Ensures no data loss in the scenarios where calculations with Datetime can be a factor. Example: if startDate = 2020-06-03, the code will calculate the number of days ago by using 2020-06-02.

11. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.
12. Click the Source Definition tab.
 - a. Click the Tokens sub-tab.
 - b. Verify token values.

The following table describes token values to verify.

Token	Value
LastRunTime	(Populated by feed)

Note: For more information about tokens, see "Data Feed Tokens" in the RSA Archer Online Documentation.

13. Verify that key field values are not missing from the data feed setup window.
14. Click Save.

Set Up the Tenable.sc Vulnerabilities RSA Archer 6.7 Data Feed


For vulnerabilities extraction, we use the vulnTool = vulnDetails in the query to make the web call to the API. This is an aggregated view of the data through the Analysis endpoint.

Important: Before you upload a JavaScript file, configure JavaScript Transporter settings in the RSA Archer Control Panel. For more information, see [Configure the JavaScript Transporter Settings](#).

Important: With the exception of the optional parameters specified in this procedure, changes to the JavaScript Transporter configuration file can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

Important: For vulnerabilities detected, RSA Archer implements with a unique key concept to associate the vulnerability detected to a specific host and a vulnerability definition. However, we understand that environment configurations are unique across an organization’s infrastructure, therefore the unique keys are configurable to each client, such as determining if a device already exists in your RSA Archer environment. And where clients have multiple scanners scanning the same set of devices or IP ranges, the unique key should be altered to a matching algorithm that identifies the device, regardless of the source. Unique key default values are as follows:

Identification of an object	Logic (configurable)
Vulnerability detected (VSR)	<p>If DNS exists, concatenate SOURCE + DNS + PLUGIN ID + PORT + PROTOCOL + REPOSITORY ID.</p> <p>If DNS does not exist, concatenate the SOURCE + PLUGIN ID + IP + PORT + PROTOCOL + REPOSITORY ID + FIRST FOUND.</p>
Device (Link Only)	Use the DNS as the match on an active Device.
Vulnerability Library definition (Link Only)	If a Plugin ID exists, create a match from the detection to the vulnerability definition.

1. Go to the Manage Data Feeds page.
 - c. From the menu bar, click  .
 - d. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the Tenable.sc_Vulnerabilities_RSA_Archer_6.7.dfx5 file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select Active.

6. In the Additional Properties section, enable Optimize Calculations.
7. Click the Transport tab.
8. In the Transport Configuration section, complete the following:
 - e. Click Upload.
 - f. From the Upload JavaScript File dialog, click Add New.
 - g. Locate and select the Signed-TenableSC_v1_0_13.js file, and click Open.
 - h. From the Upload JavaScript File dialog, click OK.
9. The JavaScript code allows clients to pass in different variables through our Custom Parameters section. The following table describes the supported values for specific Custom Parameters.

Key	Value	Description
dataSource	Only one valid value Default = hosts	
url	Requires valid value Default = [empty]	
username	Requires valid value Default = [empty]	
password	Requires valid value Default = [empty]	
proxy	Optional Default = [empty]	
vulnSeverities	Requires valid value Default = 4,3,2,1	Filter passed to the query. Eliminates unwanted vulnerability data from the query results. Data is only returned on vulnerabilities with the specified severity levels. 4 = Critical; 3 = High; 2 = Medium; 1 = Low; 0 = Informational
vulnDateFilterType	Default = firstSeen [Configurable value, but only one value allowed]	Filter passed to the query. We calculate the concept of a startDate and endDate, by using either the LastRunTime token, startDate parameter, or a default date value. The selected date is used as the filter logic passed as part of the query to eliminate unwanted vulnerabilities being returned.

Example: "filters": { "filterName": "firstSeen",
"operator": "=", "value": "#:#" }

Valid filterName values:

- **firstSeen** - Equivalent to filtering on Vulnerability Discovered on the Vulnerability Analysis page of the Tenable.sc user interface. Both the "vulnLoadActive" and "vulnLoadPatched" parameters can be used to limit the query results.
- **lastSeen** - Equivalent to filtering on Vulnerability Observed on the Vulnerability Analysis page of Tenable.sc user interface. This variable requires "vulnLoadPatched" = false.
- **lastMitigated** – Equivalent to filtering on Vulnerability Mitigated on the Vulnerability Analysis page of Tenable.sc user interface. This variable requires "vulnLoadActive" = false.

Logic to calculate the value criteria:

- First value is always = 0. This represents a value of Today, or the last possible data point that can be returned from Tenable.sc.
- The second value in the criteria is a numerical value represented by days prior to today.

ignoreLastRunTime	<p>Requires valid value</p> <p>Default = false</p>	<p>LastRunTime is a token supplied in the data feed, and by default is the date used in the query logic. In order to use startDate, the ignoreLastRunTime parameter must be set = true.</p> <p>Date Logic:</p> <ul style="list-style-type: none"> • If ignoreLastRunTime = false and LastRunTime token is empty <ul style="list-style-type: none"> ○ Default to 1970-01-10T00:00:00Z • If ignoreLastRunTime = false and LastRunTime token is not empty <ul style="list-style-type: none"> ○ Use the LastRunTime token • If ignoreLastRunTime = true and startDate is empty <ul style="list-style-type: none"> ○ Default to 1970-01-10T00:00:00Z • If ignoreLastRunTime = true and startDate is not empty <ul style="list-style-type: none"> ○ Use startDate parameter specified by client
-------------------	--	---

Tenable.sc Data Feeds for RSA Archer ITSVP 6.7

startDate	Optional Default = [empty]	Additional parameter, other than LastRunTime token, that allows clients to apply minimal, built-in search filter criteria for data extraction. An example of how the logic is applied (extraction of data is by batchSize = 1000, vulnDataFilterType = firstSeen, and startDate = 2019-04-21): <ul style="list-style-type: none"> • Calculate the "value" criteria in firstSeen. <ul style="list-style-type: none"> ○ 0:370 (ie. 4/21 = 370 days ago) • Run query using filter criteria and where startOffset=0, endOffset=1000 <ul style="list-style-type: none"> ○ Write data to file • Run query using filter criteria and where startOffset=1000, endOffset=2000 <ul style="list-style-type: none"> ○ Write data to file • Repeat the process until no data is returned from the query, indicating the final value in firstSeen criteria has been reached.
vulnLoadActive	Requires valid value Default = true [Configurable value of true or false]	Indicates whether to pull data from the Cumulative database. Also known as the Active database.
vulnLoadPatched	Requires valid value Default = true [Configurable value of true or false]	Indicates whether to pull data from the Mitigated database. Also known as Patched database.
verifyCerts	Default = false [Configurable value of true or false]	Validates the website address matches the address on the certificate, similar to browser level validation.

Important: The keys and values are case-sensitive and cannot include extra spaces at the end of the strings. The listed values are in place by default but can be configured to suit your environment.

Note: Tenable.sc treats startOffset as exclusive.

10. (Optional) The following additional parameters are valid options for the Custom Parameters section for the current JavaScript file.

Key	Value	Description
batchSize	Default = 1000 (records at a time) [Configurable]	Used for defining batches of content to be retrieved in a single call. JavaScript makes incremental calls to pull the next batch of data.
socketLimit	Default = 10 [Configurable value of 1-25]	Indicates the maximum number of open socket channels to an endpoint to be used for TCP connections.
maxRetry	Default = 1 [Configurable value of 0-2]	Indicates the amount of times a retry will occur where a "socket hung up" error is encountered. If a retry is unsuccessful and the maxRetry is exceeded, the data feed will fail.
requestsPerMin	Default = 60 [Configurable value]	A parameter to allow clients to govern the number of API requests made by RSA Archer to the external integration.
lastRunTimeOffset	Default = -1 [Configurable value]	Ensures no data loss in the scenarios where calculations with Datetime can be a factor. Example: if startDate = 2020-06-03, the code will calculate the number of days ago by using 2020-06-02.

11. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.
12. Click the Source Definition tab.
- c. Click the Tokens sub-tab.
 - d. Verify token values.

The following table describes token values to verify.

Token	Value
LastRunTime	(Populated by feed)

Tenable.sc Data Feeds for RSA Archer ITSVP 6.7

Token	Value
CrossReferencesMode	LinkOnly
RelatedReferencesMode	LinkOnly

Note: For more information about tokens, see "Data Feed Tokens" in the RSA Archer Online Documentation.

13. Verify that key field values are not missing from the data feed setup window.
14. Click Save.

Important: By leveraging a combination of the "hasBeenMitigated" and "repository" information provided by the Tenable.sc in the web call, RSA Archer is able to accurately determine whether a vulnerability is Active, Patched, or Reopened in the Scan Status field available in the Vulnerability Scan Results application.



Chapter 3: Using the Tenable.sc Data Feeds

Scheduling Data Feeds

Important: A data feed must be active and valid to successfully run.

As you schedule your data feed, the Data Feed Manager validates the information. If any information is invalid, an error message displays. You can save the data feed and correct the errors later; but the data feed does not process until you make corrections.

Note: All IT Security Vulnerabilities Program data feeds are set to run daily by default.

1. From the menu bar, click .
2. Go to the Schedule tab of the data feed that you want to modify.
 - a. From the menu bar, click .
 - b. Under Integration, click Data Feeds.
 - c. Select the data feed.
 - d. Click the Schedule tab.
3. Go to the Recurrences section and complete frequency, start and stop times, and time zone. The following table describes the fields in the Recurrences section.

Field	Description
Frequency	<p>Specifies the interval in which the data feed runs, for example, Minutely, Hourly, Daily, Weekly, Monthly, or Reference.</p> <ul style="list-style-type: none"> Minutely. Runs the data feed by the interval set. For example, if you specify 45 in the Every list, the data feed executes every 45 minutes. Hourly. Runs the data feed by the interval set, for example, every hour (1), every other hour (2) and so forth. Daily. Runs the data feed by the interval set, for example, every day (1), every other day (2) and, so forth. Weekly. Runs the data feed based on a specified day of the week, for example, every Monday of the first week (1), every other Monday (2), and so forth. Monthly. Runs the data feed based on a specified week of the month, for example, 1st, 2nd, 3rd, 4th, or Last. Recurrence. Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. For example, you can select to have a Threats data feed run immediately after your Assets data feed finishes. From the Reference Feed list, select after which existing data feed the current data feed starts. A reference data feed will not run when immediately running a data feed. The Run Data Feed Now option only runs the current data feed.
Every	Specifies the interval of the frequency in which the data feed runs.
Start Time	Specifies the time the data feed starts running.
Start Date	Specifies the date on which the data feed schedule begins.
Time Zone	Specifies the time zone in of the server that runs the data feed.

- (Optional) To override the data feed schedule and immediately run your data feed, in the Run Data Feed Now section, click Start.
- Click Save.

Appendix A: Certification Environment

Date Tested: June 2020

Product Name	Version Information	Operating System
RSA Archer	6.7	Virtual Appliance
[Partner Product]	Tenable.sc	NA