RSA® ARCHER®

Implementation Guide

# VulnDB Data Feed for RSA Archer IT Security Vulnerabilities Program

Dan Abrahamson, RSA Partner Engineering

Last Modified: February 12, 2019

RSA READY

# Solution Summary

Risk Based Security (RBS) provides detailed information and analysis on Vulnerability Intelligence, Data Breaches, and Vendor Risk Ratings. Our products, VulnDB and Cyber Risk Analytics (CRA), provide organizations access to the most comprehensive vulnerability and vendor risk knowledge bases available, including advanced search capabilities, access to raw data via RESTful API, and email alerting to assist organizations in taking the right actions in a timely manner.

VulnDB is the most comprehensive and timely vulnerability intelligence available and provides actionable information about the latest in security vulnerabilities. VulnDB allows organizations to search on and be alerted to the latest vulnerabilities, both in end-user software and the third-party libraries or dependencies that developers use to build applications. A subscription to VulnDB provides organizations with simple to understand ratings and metrics on both vendors and products, and how each contributes to the organization's risk-profile and cost of ownership.

When a new vulnerability is disclosed, organizations need to know if and where they are impacted without having to do a vulnerability scan of their environment. VulnDB contains over 65,000 additional vulnerabilities not found in the frequently relied-upon Common Vulnerabilities and Exposures (CVE) database and a much higher degree of information for each vulnerability, providing the richest, most complete vulnerability intelligence available. VulnDB helps customers better address points of risk across their organization – from application development and IT infrastructure management to security operations, vendor risk management, and procurement.

Instead of relying on legacy vulnerability scanning, the VulnDB integration with RSA Archer allows organizations to easily map vulnerability data to the assets and vendors in their environment and quickly identify if a newly disclosed vulnerability will impact them. Armed with this insight, organizations can efficiently prioritize and plan remediation activities, and also quickly identify relevant vulnerability data during security incident response activities.

## *Integration Benefits*

- Access to a richer and more timely pool of vulnerability intelligence than is available from CVE/NVD and other sources.
- Insight into vulnerabilities that could pose risk to an organization without the need for an additional vulnerability scan.
- Ability to more effectively and efficiently prioritize vulnerabilities to be remediated.

| **Partner Integration Overview** | |
|---|---|
| **RSA Archer Solution** | IT Security Vulnerabilities Program |
| **RSA Archer Use Case** | IT Security Risk Management |
| **RSA Archer Applications** | Vulnerability Library |
| **Uses Custom Application** | No |
| **Requires On-Demand License** | No |

### *Prerequisites*

A subscription to VulnDB with the API access feature is required to use the VulnDB Data Feed for Archer ITSVP.

In addition, the RSA Archer Vulnerability Library application is required for installation and operation of the VulnDB Data Feed for the RSA Archer IT Security Vulnerabilities Program use case. This application is the target for the data feed from VulnDB.

## Partner Product Configuration

### *Before You Begin*

This section provides instructions for configuring the VulnDB Data Feed for the RSA Archer IT Security Vulnerabilities Program use case. 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 VulnDB components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before 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.**

### *VulnDB and VulnDB XML Utility for RSA Archer Configuration*

Data is retrieved from VulnDB and made available for import into RSA Archer by a Python script (the "VulnDB XML Utility for RSA Archer"). The script implements the following functionality:

- Periodically fetch vulnerabilities from the VulnDB API periodically and in incremental fashion. When the script begins to run, the entire vulnerability history from VulnDB is downloaded into a set of XML files. This process can take several hours to complete. After the initial download, the utility periodically fetches new and updated vulnerabilities from VulnDB and stores those in additional XML files.
- Provides a configuration file in which VulnDB access credentials, XML file destination location, and data update intervals are specified, among other things.

The following steps must be taken to configure the VulnDB XML Utility for RSA Archer and make data available for import into RSA Archer using the Data Feed Manager:

- Create VulnDB API access credentials following the instructions in the VulnDB Portal Guide. Download the "VulnDB XML Utility for RSA Archer" from the RBS Support portal at https://riskbased.zendesk.com/hc/en-us/articles/360017443074.
- Follow the instructions in the README.md file in the download package to install and configure the VulnDB XML Utility for RSA Archer. Note that the XML file destination location must be accessible by the RSA Archer instance. The destination must also be a subdirectory of the Home Directory specified for the RSA Archer instance in the Data File Management section of the Data Feed settings in the RSA Archer Control Panel.
- Note: Be sure to change the show_cvss_v3 and package_info parameters to True if those data elements are of interest to your organization.

# RSA Archer GRC Configuration

## *RSA Archer Prerequisites*

| Components | Recommended Software |
|---|---|
| **RSA Archer** | RSA Archer 6.4 SP1 or later |
| **RSA Archer Applications** | Vulnerability Library (RSA Archer IT Security Vulnerabilities Program use case) |

Also, download the following component from the RSA Archer Exchange:

| File Name | Description |
|---|---|
| VulnDB.dfx5 | Data feed to import information from Risk Based Security's VulnDB vulnerability intelligence feed |

## *Configuration Overview*

A variety of customizations to the Vulnerability Library application are required to support the VulnDB Data Feed for RSA Archer ITSVP. First, Sub-Forms are created to organize the custom fields needed to house the VulnDB data, then the actual data fields are created in the Vulnerability Library application, and the layout of the fields on the application form is configured. Finally, the actual feed is configured to consume the VulnDB data and store it in the fields created.

### Creating Custom Sub-Forms and Associated Fields

Eight Custom Sub-Forms are required.

1. Within RSA Archer, navigate to **Application Builder > Sub-Forms**
2. Click **Add New** to create a new Sub-Form.
3. Select **Create a new Sub-Form from scratch**.
4. Enter "VulnDB Affected Products" as the name of the form and click **OK**.
5. On the **Fields** tab of the form that opens, select **Add New**.
6. Select **Create a new field from scratch,** choose **Text** as the type, and click **OK.**

7. Enter "CPE" for the Name of the field and click **Save**.
8. Repeat adding fields per the table below to create all eight Sub-Forms and the associated custom Fields. Note that fields of type "Date" should be specified as **Text Box – Date and Time** in the Display Control section of the **Options** tab when creating those fields.

**Table 1: Custom VulnDB Sub-Forms and Associated Fields**

| Sub-Form | Field Name / Type |
|---|---|
| VulnDB Affected Products | CPE / Text<br>Product Name / Text<br>Vendor Name / Text<br>Version / Text<br>VulnDB Product ID / Numeric<br>VulnDB Vendor ID / Numeric<br>VulnDB Version ID / Numeric |
| VulnDB Classifications | Description / Text<br>ID / Numeric<br>Long Name / Text<br>Name / Text |
| VulnDB Credits | Name / Text |
| VulnDB CVSSv2 Metrics | Access Complexity / Text<br>Access Vector / Text<br>Authentication / Text<br>Availability Impact / Text<br>Calculated Base Score / Numeric<br>Confidentiality Impact / Text<br>CVE ID / Text<br>Generated On / Date<br>ID / Numeric<br>Integrity Impact / Text<br>Score / Numeric<br>Source / Text |
| VulnDB CVSSv3 Metrics | Attack Complexity / Text<br>Attack Vector / Text<br>Availability Impact / Text<br>Calculated Base Score / Numeric<br>Confidentiality Impact / Text<br>CVE ID / Text<br>Generated On / Date<br>ID / Numeric<br>Integrity Impact / Text<br>Privileges Required / Text<br>Scope / Text<br>Score / Numeric<br>Source / Text<br>User Interaction / Text |

| Sub-Form | Field Name / Type |
|---|---|
| | |
| VulnDB Non-Affected Products | CPE / Text<br>Product Name / Text<br>Vendor Name / Text<br>Version / Text<br>VulnDB Product ID / Numeric<br>VulnDB Vendor ID / Numeric<br>VulnDB Version ID / Numeric |
| VulnDB Package Data | Operator / Text<br>OS / Text<br>OS Architecture / Text<br>OS Version / Text<br>Package File Name / Text<br>Package Name / Text<br>Package Version / Text |
| VulnDB References | Type / Text<br>Value / Text |

## *Creating Other Custom Fields*

1. Within RSA Archer, navigate to Application Builder > Applications.
2. Click Vulnerability Library.
3. Click the Fields tab.
4. Add custom fields corresponding to the Sub-Forms created previously. For each field, set the type to "Sub-Form", specific the corresponding Sub-Form on the General tab, and add the display fields and sort order on the Options tab.

**Table 2: Custom Vulnerability Library Sub-Form Fields**

| Field Name | Type | Display Fields | Sort Order |
|---|---|---|---|
| VulnDB Affected Products | Sub-Form | • Vendor Name<br>• Product Name<br>• Version<br>• CPE | 1. CPE – Ascending<br>2. Version - Descending |
| VulnDB Classifications | Sub-Form | • Long Name<br>• Description | 1. Long Name – Ascending<br>2. Description - Ascending |
| VulnDB Credits | Sub-Form | • Name | 1. Name - Ascending |
| VulnDB CVSSv2 Data | Sub-Form | • Source<br>• Calculated Base Score<br>• Score<br>• Access Vector<br>• Access Complexity<br>• Authentication<br>• Confidentiality Impact<br>• Integrity Impact | 1. Source - Descending<br>2. Generated On - Descending |

| Field Name | Type | Display Fields | Sort Order |
|---|---|---|---|
| | | • CVE ID<br>• Generated On | |
| VulnDB CVSSv3 Data | Sub-Form | • Source<br>• Attack Vector<br>• Attack Complexity<br>• Score<br>• Calculated Base Score<br>• Privileges Required<br>• User Interaction<br>• Scope<br>• Confidentiality Impact<br>• Integrity Impact<br>• Generated On | 1. Source - Descending<br>2. Generated On - Descending |
| VulnDB Non-Affected Products | Sub-Form | • Vendor Name<br>• Product Name<br>• Version<br>• CPE | 1. CPE – Ascending<br>2. Version - Descending |
| VulnDB Package Data | Sub-Form | • OS<br>• OS Version<br>• OS Architecture<br>• Package Name<br>• Operator<br>• Package Version<br>• Package File Name | 1. Package File Name – Ascending<br>2. Package Version - Descending |
| VulnDB References | Sub-Form | • Type<br>• Value | As desired |

Add the following custom fields with the indicated types. Again, note that fields of type "Date" should be specified as **Text Box – Date and Time** in the Display Control section of the **Options** tab when creating those fields.

**Table 3: Custom Vulnerability Library Fields – Other**

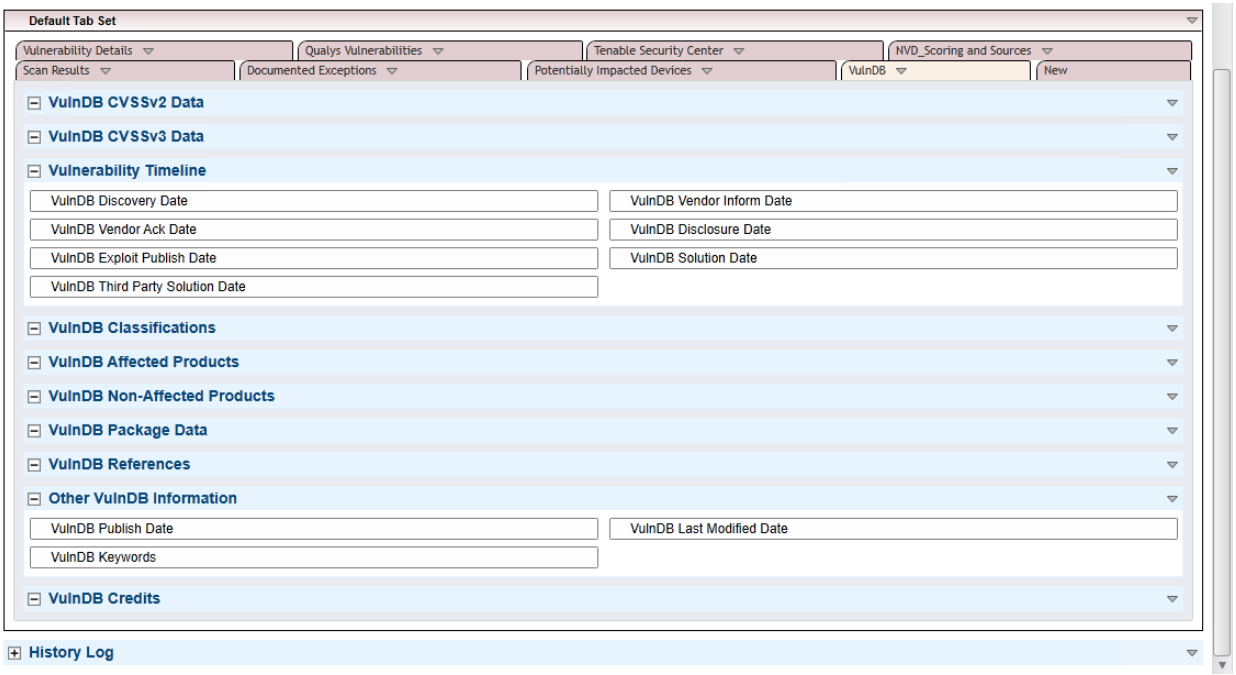
| Field Name | Type |
|---|---|
| VulnDB Disclosure Date | Date |
| VulnDB Discovery Date | Date |
| VulnDB Exploit Publish Date | Date |
| VulnDB Keywords | Text |
| VulnDB Last Modified Date | Date |
| VulnDB Publish Date | Date |
| VulnDB Solution Date | Date |
| VulnDB Third Party Solution Date | Date |
| VulnDB Vendor Ack Date | Date |
| VulnDB Vendor Inform Date | Date |

## *Configuring the Layout*

Before the VulnDB-specific fields can be displayed in RSA Archer, they need to be added to the Vulnerability Library application layout.

1. Within RSA Archer, navigate to Application Builder > Applications.
2. Click Vulnerability Library.
3. Click the Layout tab
4. Click the New tab on the Default Tab Set section and enter VulnDB for the name where prompted.
5. Add a section called "Vulnerability Timeline" by clicking Add New Layout Object, dragging Add Section to the VulnDB tab, and entering the name when prompted.
6. Add a section called "Other VulnDB Information" by clicking Add New Layout Object, dragging Add Section to the VulnDB tab, and entering the name when prompted.
7. Drag the various VulnDB Sub-Form fields onto the VulnDB tab as shown in Figure 1 below.
8. Drag the remaining VulnDB custom fields into the appropriate section on the VulnDB tab as shown in Figure 1 below.
9. Arrange the Sub-Forms and Sections as shown in Figure 1.

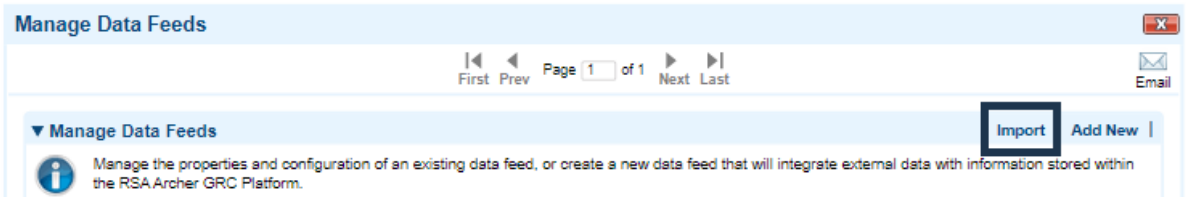
**Figure 1: VulnDB Tab Layout**



## *Import the Data Feed File*

You will need to import and configure the **VulnDB** data feed file downloaded earlier. To import the feed file, perform the following steps:

In RSA Archer, go to Integration > Data Feeds. Under Manage Data Feeds, **Import the VulnDB.dfx5 file downloaded earlier.**




1. Update the following settings on the **General Information** tab:

| Field | Value |
|---|---|
| **Status** | Active |
| **Target** | Vulnerability Library |
| **User Name** | userArcherDataFeedService (or other Archer account) |

2. Update the following settings on the **Transport** tab:
   - Set the **Transport Method** to "File Transporter"
   - Set the Path to *"VulnDBXMLFilePath"**.xml, where "*VulnDBXMLFilePath*" is the folder or share that the VulnDB Utility script is configured to store XML files. See the "VulnDB and VulnDB Utility Configuration" section earlier in this document for more information.
   - Under **Post-Processing > On Success:** select "Rename", and enter the following for the Destination Filename: {DataFileDirectoryName}\success\{DataFileName}_{Now(MM.dd.yyyy)}.{DataFileExtension}
3. On the **Navigation** tab, make sure "XML File Iterator" is selected as the **Navigation Method**.
4. Review the mappings on the **Data Map** tab. Consult **Appendix A** for more information on the predefined and recommended field mappings, including the key field definition.
5. On the Schedule tab:
   - Notice that the default is set to once a day
   - Make any changes to the schedule that you'd like
   - Click Start to pull in content immediately (optional)
6. Save the feed.

# Certification Environment for RSA Archer GRC

Date Tested: February 12, 2019

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| RSA Archer GRC | 6.5 | Virtual Appliance |
| VulnDB | | |
| | | |