RSA Archer GRC

RSA Vulnerability Risk Management

Release Notes

1.2

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: **http://www.emc.com/support/rsa/index.htm**.

Trademarks

License agreement

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

Third-party licenses

This product may include software developed by parties other than RSA.

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.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION 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.

February 2016

Contents

Preface 5
Support and Service 5
Other Resources 5
RSA Archer GRC Documentation 6
RSA Vulnerability Risk Management Documentation Set 6

Release History 8

RSA Vulnerability Risk Management 1.1 9
What's New in Release 1.1 9
Fixed Issues in Release 1.1 11

RSA Vulnerability Risk Management 1.1 SP1 12
What's New in Release 1.1 SP1 12
Fixed Issues in Release 1.1 SP1 14

RSA Vulnerability Risk Management 1.1 SP1 P1 15
What's New in Release 1.1 SP1 P1 15
Fixed Issues in Release 1.1 SP1 P1 15
Installing RSA Vulnerability Risk Management 1.1 SP1 P1 15
Install RSA Vulnerability Risk Management 1.1 SP1 P1 16

RSA Vulnerability Risk Management 1.1 SP1 P2 17
Fixed Issues in Release 1.1 SP1 P2 17
Installing RSA Vulnerability Risk Management 1.1 SP1 P2 17
Install RSA Vulnerability Risk Management 1.1 SP1 P2 18

RSA Vulnerability Risk Management 1.1 SP1 P3 20
Fixed Issues in Release 1.1 SP1 P3 20
Install RSA Vulnerability Risk Management 1.1 SP1 P3 20

RSA Vulnerability Risk Management 1.1 SP1 P4 22
What's New in Release 1.1 SP1 P4 22
Fixed Issues in Release 1.1 SP1 P4 23
Install RSA Vulnerability Risk Management 1.1 SP1 P4 23

RSA Vulnerability Risk Management 1.1 SP1 P5 26
Fixed Issues in Release 1.1 SP1 P5 26
Install the RSA Vulnerability Risk Management 1.1 SP1 P5 26

RSA Vulnerability Risk Management 1.2 28
What's New in Release 1.2 28
Fixed Issues in Release 1.2 28

Known Issues 31

Documentation Errata 34
Troubleshooting 34

Documentation Supplement 35
Add the Tenable Nessus v6 Endpoint 35
Enable Scan Reports and Vulnerabilities for Tenable Nessus v6 36

Preface

This document lists what's new and changed in RSA® Vulnerability Risk Management.

These *Release Notes* may be updated. The most current version can be found on RSA SecurCare® Online at **https://knowledge.rsasecurity.com**.

The audience for this document is the RSA Archer administrator.

Support and Service

Customer Support Information	**www.emc.com/support/rsa/index.htm**
Customer Support E-mail	**archersupport@rsa.com**

Other Resources

RSA Archer Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide RSA Archer product roadmap. **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**

RSA Archer Exchange is an online marketplace dedicated to supporting GRC initiatives that delivers on-demand applications with service, content, and integration providers to drive the success of RSA Archer clients. **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**

RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with instructions and other information about interoperation of RSA products with these third-party products. **https://gallery.emc.com/community/marketplace/rsa/**

RSA SecurCare Online (SCOL) provides unlimited access to a wealth of resources on the Web, 24 hours a day. The secure system provides members access to a support knowledgebase, to download current platform patches and bug fixes, to sign up for notifications, to manage your support cases and more. **https://knowledge.rsasecurity.com/**

RSA Archer GRC Documentation

You can access the RSA Archer GRC documentation from the RSA Archer Exchange and RSA Archer Community.

Documentation	Location
Platform, Solutions, Applications, and Content	On the RSA Archer Community at: **https://community.rsa.com/community/products/ArcherGRC**

RSA continues to assess and improve the documentation. Check the RSA Archer Community for the latest documentation.

RSA Vulnerability Risk Management Documentation Set

For information about the RSA Vulnerability Risk Management solution, see the following documentation:

Guide	Description
RSA Vulnerability Analytics Help	Provides users and administrators with instructions on how to use the RSA Vulnerability Analytics UI.
Installation and Configuration Guide	Provides administrators with instructions on how to install and configure the solution.
Practitioner Guide	Provides design information about the solution and a use case highlighting how the solution works.
Release Notes	Introduces the RSA Vulnerability Risk Management solution, lists the documentation available, and provides information for obtaining support and service.
Upgrade Guide	Provides administrators with instructions on upgrading their existing RSA VRM setup.
Backup and Recovery Guide	Provides administrators with instructions on backing up and recovering their RSA VRM setup.
RSA Vulnerability Analytics Search API Guide	Provides administrators with instructions on using the RSA VA Search API. **Note:** This is included in the RSA Vulnerability Analytics Help.

Guide	Description
Extensions Guide	Provides administrators with instructions on configuring various extensions with which RSA VRM can be setup.
ACME Corp Sizing Guide	Provides detailed information about performance and sizing measurements pertaining to common business activities performed with RSA Vulnerability Risk Management.

You can access the RSA Vulnerability Risk Management solution documentation from the Documents page on the RSA Archer Exchange at **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange** or on RSA SecurCare® Online at **https://knowledge.rsasecurity.com/**.

Release History

Version	Date	Description
1.1	June 2014	Release
1.1 SP1	December 2014	Service Pack Release
1.1 SP1 P1	January 2015	Patch Release
1.1 SP1 P2	April 2015	Patch Release
1.1 SP1 P3	August 2015	Patch Release
1.1 SP1 P4	November 2015	Patch Release
1.1 SP1 P5	January 2016	Patch Release
1.2	March 2016	Release

RSA Vulnerability Risk Management 1.1

This document introduces RSA© Vulnerability Risk Management 1.1. Read this document before installing the software. This document contains the following sections:

- **What's New in Release 1.1**
- **Fixed Issues in Release 1.1**

What's New in Release 1.1

This section describes the major changes introduced in this release.

Feature	Description
Installation	RSA Vulnerability Risk Management is now updated to version 1.1.
Support for Custom CSV and XML Imports	RSA Vulnerability Risk Management now supports custom .csv and .xml file imports.
Support for Tenable Nessus	RSA Vulnerability Risk Management now supports Tenable Nessus as an endpoint configuration.
Support for Rapid7	RSA Vulnerability Risk Management now supports Rapid7 as an endpoint configuration.
RSA Archer GRC Platform 5.5 Support	RSA Vulnerability Risk Management 1.1 now works with the RSA Archer Platform 5.4 SP1 and 5.5.
RSA Security Analytics Warehouse 10.3 SP2 Support	RSA Vulnerability Risk Management 1.1 now works with the RSA Security Analytics Warehouse 10.3 SP2.
Historical Metrics Within RSA Vulnerability Analytics	Reports within RSA Vulnerability Analytics can now include historical metrics over a specified period of time, such as monthly, weekly, and daily.
Search Query Syntax Assistance	The search query syntax is now color coded based upon the elements involved. Additionally, fields can be automatically selected using partial spelling results.
New Tickets UI	Tickets are now listed by the due date. Clicking on each record

Feature	Description
	displays the ticket details on the right side of the page.
Easily Select All Visible Rows for Vulnerability and Device Searches	You can now mass select all currently visible rows during vulnerability and device searches.
Pagination Enabled for Issue Searches	When searching for issues, you can search through pages that include 200 issues at a time. When switching to a new page, any previously selected issues become unselected.
General History/Back/Refresh Support for UI Pages	If you open a search page or the details page of a record and then navigate to a different page, the history saves and can be returned to at a later time.
Enable or Disable Specific Rules	You can now manually enable or disable specific rules in the Rules Administration page.
Merged Record Drop-down	If a record is imported from multiple sources, they are now combined into a single record with a drop-down list to review the details from each source.
Easier Issue Searches	When reviewing details for a Device or Vulnerability, you can now click the Number of Open Issues field, which leads you to the Issues tab with the selected device or vulnerability pre-populated in the search box.
Navigation Menu Changes	The Data Warehouse, Rules, Users, and Device Groups pages are now found under the Administration menu.
Search Performance Optimization	If an Issue, Vulnerability, or Device search results in 1,000,000 matches or more, a notification displays when you scroll to the bottom of the list prompting you to narrow your search criteria.

Fixed Issues in Release 1.1

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Data Collector	ITSRM-429	The VRM Data Collector service may hang if stopped from the Service Panel.
Data Collector	ITSRM-568	After making configuration changes, the changes doesn't take effect until the Data Collector service is restarted.
Data Collector	ITSRM-1473	After making RVDW configuration changes, the changes doesn't take effect until the Data Collector service is restarted.
Data Collector	ITSRM-1860	When running ETL jobs, text in formats other than UTF-8 may not be recognized.
Data Collector	ITSRM-1865	NVD jobs create a file called getAllVulnerabilitiesError.log in the C:\tmp\nvd folder.
Data Collector	ITSRM-1991	If you restart the Data Collector service while the Connection Manager is open, the Connection Manager fails to run.
Installer	ITSRM-1870	The setup-vrm-data.sh script fails if it is not executed from the /opt/rsa/vrm/setup directory.
Web-Reporting	ITSRM-1835	When adding new charting options to RSA Vulnerability Analytics reports, the chart colors change each time.
Web-Tickets	ITSRM-1995	If you try to change the assignee for a ticket, but do not specify who, the ticket is assigned to no one.

RSA Vulnerability Risk Management 1.1 SP1

This document introduces RSA Vulnerability Risk Management 1.1 SP1. Read this document before installing the software. This document contains the following sections:

- **What's New in Release 1.1 SP1**
- **Fixed Issues in Release 1.1 SP1**

What's New in Release 1.1 SP1

This section describes the major changes introduced in this release.

Feature	Description
Installation	RSA Vulnerability Risk Management is now updated to version 1.1 SP1.
Enhanced Support for Rapid7	RSA Vulnerability Risk Management now supports Rapid7 5.10.2 and 5.11.6 as endpoint configurations.
RSA Archer GRC Platform 5.5 Support	RSA Vulnerability Risk Management 1.1 SP1 now works with the RSA Archer Platform 5.4 SP1 P1 and 5.5 SP2.
RSA Analytics Warehouse (MapR) Support	RSA Vulnerability Risk Management 1.1 SP1 now works with the RSA Analytics Warehouse 10.3 SP4 and 10.4 P2.
Historical Metrics Workflow Within RSA Vulnerability Analytics	Historical Metrics within RSA Vulnerability Analytics can now be automatically run over a specified period of time, such as monthly, weekly, and daily.
Individual Endpoint Proxy Support	Individual endpoints can now be configured to use a proxy server.
Cron Scheduler Assistance	When creating Cron schedules within RSA Vulnerability Analytics rules, an automated Cron scheduler now writes the Cron schedule in the correct format for you.
Ticket Splitting Based on Devices and Vulnerabilities	You can now split RSA Vulnerability Analytics tickets into just Devices or Vulnerabilities when sending the ticket to RSA Archer.
Configurable Issue	You can now configure how many issues you can view and

Feature	Description
Selection Limit	select at one time within RSA Vulnerability Analytics.
Single Sign-On Support	You can now access RSA Vulnerability Analytics through single sign-on with Site Minder.
Easily Select All Visible Rows for Vulnerability and Device Searches	You can now mass select all currently visible rows during vulnerability and device searches.
Performance Enhancements	RSA Vulnerability Analytics has been optimized for increased performance.
Role Based Access Control Support	RSA Vulnerability Analytics now supports role-based access control with three separate access levels.
HBase Backup and Recovery	RSA Vulnerability Risk Management 1.1 SP1 now supports backing up and recovering HBase tables.
Instant RSA Archer Sync for New Findings	When sending a Finding to RSA Archer, RSA Vulnerability Analytics now syncs immediately with RSA Archer.
Stored Issue State Counts in Findings	You can now view a count of the various issue states that are present in an RSA Archer Finding within RSA Archer.
Daily Spreadsheet Updates	The spreadsheet attached to the RSA Archer Finding is now updated daily to show the previous day’s progress.
Custom Field Globally Unique Identifier (GUID) Overrides	The Field GUIDs within the RSA Archer Vulnerability Risk Management solution can now be overridden with custom GUID values.
Documentation Set Additions	The RSA Vulnerability Risk Management 1.1 SP1 documentation set now includes a Backup and Recovery Guide, an Upgrade Guide, a Search API Guide, and an Extensions Guide.

Fixed Issues in Release 1.1 SP1

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Archer Data Integration	ITSRM-1968	Any tickets that are granted a very long exception always stay in the Open state.
Archer Data Integration	ITSRM-2024	If a device in RSA Vulnerability Analytics does not have an associated Device Type, the device record cannot be pushed to RSA Archer.
Archer Solution	ITSRM-1969	In the RSA Archer Vulnerability Risk Management solution, the Exceptions by Submitter report only shows exceptions with the risk rating of High.
Data Collector	ITSRM-2656	When using the Edit Endpoint option in the Connection Manager, the updates do not take effect until the Data Collector service is restarted.
Rules	ITSRM-1912	After editing field aliases, the change does not take effect until both the Web UI and Data Collector services are restarted.
Web- Devices	ITSRM-2810	Devices could not be synchronized between RSA Archer VRM and RSA VA.
Web- Issues	ITSRM-2644	Sometimes, the CVSS Final Score displayed in RSA Vulnerability Analytics does not match the actual CVSS score for issues imported through Rapid7 or Nessus.
Web- Search	ITSRM-2017	If you try to search facet values using the NOT operation, the search query does not complete.
Web- Vulnerability	ITSRM-1651	Recent edits to a large number of entries may not refresh properly.
Web- Vulnerability	ITSRM-1817	When sorting by overall score, "0.0" values are mixed with "NULL" values.

RSA Vulnerability Risk Management 1.1 SP1 P1

This document introduces RSA Vulnerability Risk Management 1.1 SP1 P1. Read this document before installing the software. This document contains the following sections:

- What's New in Release 1.1 SP1 P1
- Fixed Issues in Release 1.1 SP1 P1

What's New in Release 1.1 SP1 P1

Feature	Description
Issue Score	Issue Scores are now calculated using the individual vulnerability source which provides a more accurate score. **Note:** The new scoring logic will not be enabled until scan results are ingested for any issues that were already loaded in the system when the Patch was installed.

Fixed Issues in Release 1.1 SP1 P1

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Data Collector	ITSRM-3247	Rapid7 vulnerability definitions no longer fail due to malformed XML.
Web Devices	ITSRM-3241	Unmatched devices no longer count against the IP limit for licensing.

Installing RSA Vulnerability Risk Management 1.1 SP1 P1

The RSA Vulnerability Risk Management patch is installed on the RSA Vulnerability Analytics Windows Host and does not require any changes to the cluster.

The following file is included in the patch:

- rsa-vrm-1.1.1.xx-patch-installer.exe

Install RSA Vulnerability Risk Management 1.1 SP1 P1

Important: The patch can only be installed on a machine on which RSA Vulnerability Risk Management 1.1 SP1 is installed and fully functional.

Procedure

1. Log in to the Windows Host Server with Administrator access.
2. Stop the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services.
3. If data is already loaded in the RSA Vulnerability Risk Management system, do the following:
   a. On any node of the cluster, clear cached files by running the following command:
      ```
      hadoop fs -rmr /user/vrm/dependencies
      ```
   b. In the collector-config.properties files, for all configured endpoints, set vulnerability job lastTimeRun values to 0.
4. Double-click the rsa-vrm-1.1.1.xx-patch-installer.exe installation file.
5. Complete the installation using the installation wizard.
6. Verify that the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services have been restarted.
7. Run the vulnerability jobs.

RSA Vulnerability Risk Management 1.1 SP1 P2

This document introduces RSA Vulnerability Risk Management 1.1 SP1 P2. Read this document before installing the software. This release contains the following section:

- **Fixed Issues in Release 1.1 SP1 P2**
- **Installing RSA Vulnerability Risk Management 1.1 SP1 Patch 2**
- **Install RSA Vulnerability Risk Management 1.1 SP1 Patch 2**

Fixed Issues in Release 1.1 SP1 P2

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Archer Solution, Data Collector	ARCHCE-1065	The GetFindings job fails to push an RSA Archer Findings record back to RSA Vulnerability Analytics when the Due Date has been updated.
Data Collector	ARCHCE-618	The RSA Archer Lookup Workflow ETL job fails when there are more than 50 items in the Platform and Type Values List fields in the Device Application.
Data Collector	ARCHCE-1289	McAfee scan sets the End Date of the job to the current time even though the scan is not yet complete.
Web -Search	ARCHCE-1430	Two buttons on the RSA Vulnerability Analytics search page are both named Search, but function differently.
Web- Tickets	ARCHCE-1270	If clicking the Ticket Details in an RSA Archer Finding record requires a login to RSA Vulnerability Analytics (RSA VA), then after logging in to RSA VA, the user lands on the wrong page.

Installing RSA Vulnerability Risk Management 1.1 SP1 P2

The RSA Vulnerability Risk Management patch requires that you install the RSA Vulnerability Analytics installer on the Windows Host, and upgrade the RSA Vulnerability Risk Management solution on the RSA Archer Server. The patch does not require any changes to the cluster.

The following files are included in the patch:

- rsa-vrm-1.1.1.xx-patch-installer.exe
- RSA_Vulnerability_Risk_Management_v1.1_SP1_P2.zip

Install RSA Vulnerability Risk Management 1.1 SP1 P2

Important: The patch can only be installed on a machine on which RSA Vulnerability Risk Management 1.1 SP1 or RSA Vulnerability Risk Management 1.1 SP1 P1 is installed and fully functional.

Procedure

1. Install the RSA Vulnerability Risk Management solution. For more information, see "Install the RSA Vulnerability Risk Management Solution" and "Post Install Activities" in the *RSA Vulnerability Risk Management 1.1 SP1 Installation and Configuration Guide*.
2. To verify that RSA Vulnerability Risk Management upgraded successfully, do the following:
   a. In the Findings application, click the Calculations tab.
   b. Verify that the following fields are listed in the following order:
      - Year
      - Status Prior Value
      - Status
      - Status Change
      - Expected Remediation Date
      - Actual Remediation Date
      - Remediation Status
      - Source
      - Default Record Permissions
      - Inherited Record Permissions
      - Criticality (Text)
      - Assigned to
      - Reviewer
      - State
      - Due Date Previous Value

   - Due Date
   - Count of Exception Requests
   - Response Status
   - Days of Approval
   - Days Overdue
   - Ticket Details (Link to VA)
   - Total Number of Open Issues
   - Total Number of Closed Issues
   - VRM Process Record Flag

3. Install the RSA Vulnerability Analytics Host. For more information, see "Install the RSA Vulnerability Analytics User Interface" in the *RSA Vulnerability Risk Management 1.1 SP1 Installation and Configuration Guide*.
4. Log in to the Windows Host Server with Administrator access.
5. Stop the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services.
6. If data is already loaded in the RSA Vulnerability Risk Management system, do the following:

   a. On any node in the cluster, clear all cached files by running the following command:

   ```
   hadoop fs -rmr /user/vrm/dependencies
   ```

   b. In the collector-config.properties file, for all configured endpoints, set vulnerability job lastTimeRun values to 0.

7. Double-click the rsa-vrm-1.1.1.xx-patch-installer.exe installation file.
8. Complete the installation using the installation wizard.
9. Verify that the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services have been restarted.
10. Run the vulnerability jobs.

RSA Vulnerability Risk Management 1.1 SP1 P3

This document introduces RSA Vulnerability Risk Management 1.1 SP1 P3. Read this document before installing the software. This release contains the following sections:

- **Fixed Issues in Release 1.1 SP1 P3**
- **Install RSA Vulnerability Risk Management 1.1 SP1 P3**
- **Documentation Errata**

Fixed Issues in Release 1.1 SP1 P3

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Data Collector	ARCHCE-1259	Timezone setting is missing in the job, so it picks up the default timezone of the environment, which is inconsistent with the design.
Data Collector	ARCHCE-1502	Log errors occur when the custom data workflow with backup is running correctly.
Data Collector	ARCHCE-1504	Custom endpoint workflow does not re-index assets after loading scan results.
Data Collector	ARCHCE-1734	The validation of last modified time versus last run time is not necessary for the custom workflow.
Web -Search	ARCHCE-1412	Search only goes through UI cache for certain browsers (IE, Firefox).
Web- Tickets	ARCHCE-2237	The VA Tickets tab does not show the complete count of tickets retrieved.

Install RSA Vulnerability Risk Management 1.1 SP1 P3

The RSA Vulnerability Risk Management patch requires that you install the RSA Vulnerability Analytics installer on the Windows Host. The patch does not require any changes to the cluster.

The following file is included in the patch:

- rsa-vrm-1.1.1.xx-patch-installer.exe

Important: The patch can only be installed on a machine on which RSA Vulnerability Risk Management 1.1 SP1, 1.1 SP1 P1, or 1.1 SP1 P2 is installed and fully functional. If upgrading from 1.1 SP1 or 1.1 SP1 P1, you must download and install the RSA_Vulnerability_Risk_Management_v1.1_SP1_P2.zip solution package before upgrading to 1.1 SP1 P3.

To obtain the RSA Vulnerability Risk Management 1.1 SP1 P2 solution package, log on to RSA SecurCare Online at https://knowledge.rsasecurity.com and click Products in the top navigation menu. Select "RSA Archer GRC" and the "Version Upgrades" link. Under the "Version Upgrade" table, select "Archer Platform" then the "Download Software" button to take you to Download Central for the latest RSA Archer GRC versions. For information on installing the solution package, see **Install RSA Vulnerability Risk Management 1.1 SP1 P2**.

Procedure

1. Stop the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services.
2. If data is already loaded in the RSA Vulnerability Risk Management system, do the following:
   a. On any node in the cluster, clear all cached files by running the following command:

      ```
      hadoop fs -rmr /user/vrm/dependencies
      ```

   b. In the collector-config.properties file, for all configured endpoints, set vulnerability job lastTimeRun values to 0.
3. Double-click the rsa-vrm-1.1.1.xx-patch-installer.exe installation file.
4. Complete the installation using the installation wizard.
5. Verify that the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services have been restarted.
6. Run the vulnerability jobs.

RSA Vulnerability Risk Management 1.1 SP1 P4

This document introduces RSA Vulnerability Risk Management 1.1 SP1 P4. Read this document before installing the software. This release contains the following sections:

- **What's New in Release 1.1 SP1 P4**
- **Fixed Issues in Release 1.1 SP1 P4**
- **Known Issues**
- **Install RSA Vulnerability Risk Management 1.1 SP1 P4**
- **Documentation Supplement**

What's New in Release 1.1 SP1 P4

Feature	Description
Data Collector	RSA Vulnerability Risk Management now supports NIST server changes to the National Vulnerability Database (NVD) website introduced on October 16th, 2015.
Rules	The maximum length for saved rules and queries in Vulnerability Analytics has been increased to 8096 characters.
Tenable Nessus v6 Support	RSA Vulnerability Risk Management now supports Tenable Nessus v6 through a new endpoint and workflow logic. To enable Nessus v6, see **Add the Tenable Nessus v6 Endpoint** and **Enable Scan Reports and Vulnerabilities for Tenable Nessus v6**.

Fixed Issues in Release 1.1 SP1 P4

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Data Collector	ARCHCE-2175 SF-00706933	Issues from Authenticated, Unauthenticated, and Authorized Qualys Scans from the same device are logged as the same issues during subsequent scans.
Data Collector	ARCHCE-2486 SF-00705474	Invalid assignedTo Value error in the collector log appears for Update Finding Workflow.
Data Collector	ARCHCE-2883	The username and password in the URL request is encoded for Tenable Nessus 6.
SAW/hBase	ARCHCE-2007, 2733 SF-00681369	The Schema setting for Issues and Devices is incorrect. RSA Archer applications display as multiple issues in VRM.
Security	ARCHCE-2796	VRM UI fails to load in Chrome browser v45 or later due to changes to Chrome v45 and later which block access to pages with weak ephemeral Diffie-Hellman keys.
Web-Tickets	ARCHCE-2478 SF-00701293	The Tickets tab in Vulnerability Analytics does not show the complete count of retrieved tickets.

Install RSA Vulnerability Risk Management 1.1 SP1 P4

The RSA Vulnerability Risk Management 1.1 SP1 P4 patch requires that you install the RSA Vulnerability Analytics installer on the Windows Host and upgrade the RAW cluster.

The following files are included in the patch:

- rsa-vrm-1.1.1.xx-patch-installer.exe
- vrm-1.1.1-xx.tar

Important: The patch can only be installed on a machine on which RSA Vulnerability Risk Management 1.1 SP1, 1.1 SP1 P1, 1.1 SP1 P2 or 1.1SP1 P3 is installed and fully functional. If upgrading from 1.1 SP1 or 1.1 SP1 P1, you must download and install the RSA_Vulnerability_Risk_Management_v1.1_SP1_P2.zip solution package before upgrading to 1.1 SP1 P4.

Procedure

1. If you currently have RSA Vulnerability Risk Management 1.1 SP3 installed and fully functional on the machine, go to step 2. Otherwise, you must install RSA Vulnerability Risk Management 1.1 SP1 or later.

   To obtain the RSA Vulnerability Risk Management 1.1 SP1 P2 solution package, log on to RSA SecurCare Online at https://knowledge.rsasecurity.com and click Products in the top navigation menu. Select "RSA Archer GRC" and the "Version Upgrades" link. Under the "Version Upgrade" table, select "Archer Platform" then the "Download Software" button to take you to Download Central for the latest RSA Archer GRC versions. For information on installing the solution package, see **Install RSA Vulnerability Risk Management 1.1 SP1 P2**.

2. Log in to the Windows Host Server with Administrator access.
3. Stop the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services.
4. If data is not already loaded in the system, go to step 6. If data is already loaded in the system, go to step 6. If data is already loaded in the RSA Vulnerability Risk Management system, do the following:
   a. On any node in the cluster, clear all cached files by running the following command:

      ```
      hadoop fs -rmr /user/vrm/dependencies
      ```

   b. In the collector-config.properties file, for all configured endpoints, set vulnerability job lastTimeRun values to 0.
5. Double-click the rsa-vrm-1.1.1.xx-patch-installer.exe installation file.
6. Complete the installation using the installation wizard.
7. Verify that the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services have been restarted.
8. Upgrade the RAW cluster, as follows:
   a. On the first node in the RAW cluster, copy vrm-1.1.1-xx.tar to the /tmp directory.
   b. With root user access, enter the following command:

      ```
      cd /tmp
      tar xvf vrm-1.1.1-xx.tar
      ```

   c. Start the automated upgrade script by running the following commands:

      ```
      cd /tmp/vrm-1.1.1
      ./rsa-vrm-1.1.1.4-upgrade.sh
      ```

Important: You may be prompted for root passwords for remote nodes. Do not leave the upgrade unattended as prompts for the root passwords may time out. If timeout occurs, repeat step 9.

9. In Connection Manager, run the Solr Reindex workflow, as follows:
   a. Enter the number for Run Workflow.
   b. Enter the number for Run Workflow for Build in Jobs.
   c. Enter the number for Run Workflow for Build in Jobs: Default.
   d. Enter the number for Run Workflow Built in Jobs: Default: solr.
10. In Connection Manager, run the vulnerability jobs for each scanner.

RSA Vulnerability Risk Management 1.1 SP1 P5

This document introduces RSA Vulnerability Risk Management 1.1 SP1 P5. Read this document before installing the software. This release contains the following sections:

- **Fixed Issues in Release 1.1 SP1 P5**
- **Install the RSA Vulnerability Risk Management 1.1 SP1 P5**

Fixed Issues in Release 1.1 SP1 P5

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Archer Data Integration	ARCHCE-1570	In the VRM Findings application, the Source field calculation needs to changed in order to avoid the empty value conduction and resulting null pointer exception in the MapR job tracker.
Data Collector	ARCHCE-3051	When importing a file from the Tenable Nessus Manager, a VA server error occurs. This is a result of the VA Talend job pulling Nessus results before the scan completes.
Data Collector	ARCHCE-2805	The Update Findings Workflow is producing a large number of files into an incoming directory of the Data Collector.

Install the RSA Vulnerability Risk Management 1.1 SP1 P5

The RSA Vulnerability Risk Management patch requires that you install the RSA Vulnerability Analytics installer on the Windows Host. The patch does not require any changes to the cluster.

The following file is included in the patch:

- rsa-vrm-1.1.1.xx-patch-installer.exeinstaller.exe

Important: This patch can only be installed on a machine that has RSA VRM 1.1 SP1, 1.1 SP1 P1, 1.1 SP1 P2, 1.1SP1 P3 or 1.1 SP1 P4 installed and fully functional. If you are upgrading from RSA VRM 1.1 SP1 or 1.1 SP1 P1, you must download and install the RSA_Vulnerability_Risk_Management_v1.1_SP1_P2.zip package before upgrading to RSA VRM 1.1 SP1 P5.

Procedure

1. If you currently have RSA VRM 1.1 SP1 P4 installed and fully functional on your machine, continue to step 2.

   Otherwise, you must install RSA VRM 1.1 SP1 P4 first.

   Note: The RSA Analytics Warehouse only needs to be upgraded if you are upgrading from RSA VRM 1.1 SP1, 1.1 SP1 P1, 1.1 SP1 P2 or 1.1 SP1 P3. For RAW upgrade instructions, go to **Install RSA Vulnerability Risk Management 1.1 SP1 P4** and complete steps 8-10.

   To obtain the RSA Vulnerability Risk Management 1.1 SP1 P2 solution package, log on to RSA SecurCare Online at https://knowledge.rsasecurity.com and click Products in the top navigation menu. Select "RSA Archer GRC" and the "Version Upgrades" link. Under the "Version Upgrade" table, select "Archer Platform" then the "Download Software" button to take you to Download Central for the latest RSA Archer GRC versions. For information on installing the solution package, see **Install RSA Vulnerability Risk Management 1.1 SP1 P2**.

2. Log into the Windows Host Server with Administrator access.

3. Stop the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services.

4. If data is not already loaded in the system, go to step 6. If data is already loaded in the RSA Vulnerability Risk Management system, do the following:

   a. On any node in the cluster, clear all cached files by running the following command:

   ```
   hadoop fs -rmr/user/vrm/dependencies
   ```

   b. In the collector-config.properties file, set the vulnerability job lastTimeRun values to 0 for all of the configured endpoints.

5. Double-click the rsa-vrm-1.1.1.xx-patch-installer.exe installation file.

6. Complete the installation using the installation wizard.

7. Verify that the RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface services have been restarted.

RSA Vulnerability Risk Management 1.2

This document introduces RSA Vulnerability Risk Management 1.2. Read this document before installing the software. This release contains the following sections:

- **What's New in Release 1.2**
- **Fixed Issues in Release 1.2**

What's New in Release 1.2

This section describes the major changes introduced in this release.

Feature	Description
Map Reduce Jobs	MapR 4.1 upgrade is included and support for JRE 1.8
Workflow	Support for Tenable Security Center.
Web - Browser Support	Updated Ext-Js to the latest version.
Data Collector	Embedded components, JRE, Jetty Server, and 3rd party dependencies, are updated to the latest version.

Fixed Issues in Release 1.2

This section describes issues that were resolved in this release.

Component	Tracking ID	Description
Map Reduce Jobs	ITSRM-3402	The way Issue Records calculate the Score and Source Metrics (description, solution, CVSS metrics, etc) has changed when an Issue goes into the verified state. It would previously fall back to the merged view of the vulnerability and use scores/etc from that. Now, it keeps the values from the "last opened" source vuln in order to view what was fixed.
Installer	ITSRM-3316	On Windows Server 2012 R2 Standard, the RSA Vulnerability Management - Data Collector service stops abruptly. You must re-install the runtime environment using 64-bit architecture.
Data Collector	ITSRM-2598	The Data Collector service cannot be stopped while a job is in progress.
Administration, Dashboard	ITSRM-3021	Users are able to enter HTML text in certain text boxes causing html injection.
Security	ITSRM-3140	SSH private keys used by VRM for root access between nodes are stored unencrypted on the file system.
Installer	ITSRM-3242	Running vrm-install.sh on the cluster wipes the rest of the iptables' rules when iptables service is stopped.
Workflow	ITSRM-3249	The Rapid7 workflow job sometimes fails due to memory issues.
Workflow	ITSRM-3296	Rapid7 jobs sometimes fail with SSLHandshake exceptions.
Installer	ITSRM-3317	The Data Collector service does not start when using Windows 2012 R2 standard.
Web - Tickets	ITSRM-3328	The Ticket Information panel shows the last query's ticket details when the query returns no records.
Workflow	ITSRM-3374	Historical Metrics are not pushed to Archer.
Installer	ITSRM-3375	Upgrade fails if services were not stopped pre-upgrade.

Component	Tracking ID	Description
Installer	ITSRM-3389	The UI and Collector Window Services have recovery options enabled, which restarts the services if the user manually tries to stop them.
Installer	ITSRM-3392	If the connection manager is open during an upgrade, the upgrade fails.
Web - Issues	ITSRM-3441	Issue rules' change attribute rule action does not allow 3-digit days.
Archer, Usability	ITSRM-3451	The 'Issue State' report in Archer adds up all the data for all the days instead of showing the current day's state.
Map Reduce Jobs, PSR	ITSRM-3447	If some of devices do not have related vulnerability IDs, the MapR job fails.
Data Collector	ITSRM-3352	If a proxy is used for adding the Tenable Nessus endpoint, Tenable Nessus certificates are not added to the VRM truststore.
Data Collector, Installer	ITSRM-3417	The Data Collector service does not start if there is a new build/version of JRE installed on the VA host.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it has been noted or referenced in detail. For many of the workarounds in this section, you must have administrative privileges. If you do not have the required privileges, contact your administrator.

Tracking ID	Description	Workaround
ARCHCE-1597	When a ticket in RSA Vulnerability Analytics is in an Active state, the Due Date is not updated.	No workaround currently exists.
ITSRM-1497	If there is network connectivity loss between the web server and the RAW, report charting options are unselectable.	Restart the web server.
ITSRM-1899	If the RSA Archer GRC user credentials used for configuring the RSA Archer GRC endpoint are expiring soon, the connection manager may fail to connect.	If the ETL job for RSA Archer GRC succeeds on the SOAP connection, but fails the REST connection, change the RSA Archer user account password.
ITSRM-1939	If at any time a corrupted file gets into the system, and the MapReduce loading job fails, the system leaves the file as is. The next time the job executes, the system finds this file and tries to load it again, resulting in the same error.	Locate and clear out any corrupted data files that consistently fail.
ITSRM-1978	The Administrator field in RSA Vulnerability Analytics shows up in RSA Archer GRC as the Device Manager field instead of the Administrator field.	No workaround currently exists.
ITSRM-2455	After clicking on a dashboard alert for a device, vulnerability, or issue, the Devices, Vulnerabilities, or Issues page may be blank.	Refresh the Devices, Vulnerabilities, or Issues page.

Tracking ID	Description	Workaround
ITSRM-2705	When a proxy server is required, certificates do not install automatically.	Manually install the certificate. Perform the following procedure: 1. Set up the proxy configuration in the Connection Manager. 2. Install the certificates manually (see the McAfee setup in Appendix A of the *RSA Vulnerability Risk Management 1.1 Installation and Configuration Guide*). **Important:** If you are installing multiple certificates, they must be added one at a time, and they must be located in different directories. 3. Add the endpoint in the Connection Manager, ignoring any errors about installing certificates. 4. Restart the Data Collector service.
ITSRM-3097	Once set to Reopened, Fixed and Verified issues that are a part of Closed tickets cannot be bundled into new Tickets through rules.	No workaround currently exists.
ITSRM-3221	When trying to create a new rule from the Issues/Vulnerabilities/Devices or Tickets windows, the window is too big. This causes issues where the Save and Cancel buttons are either missing or barely visible.	Re-size the Rule Creation window.
ITSRM-3250	For some issues, the issue score calculation is off by one decimal point.	No workaround currently exists.

Tracking ID	Description	Workaround
ITSRM-3252	When there are null values for some of the base and temporal metrics in the source vulnerability that has the highest overall score, the merged vulnerability displays the metrics of another source vulnerability instead of null values.	No workaround currently exists.
ITSRM-3263	Issue Metrics for Authentication Required and PCI Flag are incorrectly displayed when null.	No workaround currently exists.
ITSRM-3265	On the Issue Details page, all of the source vulnerabilities on a device are displayed, including fixed vulnerabilities.	No workaround currently exists.
ITSRM-3269	When the single scanner finds multiple source vulnerabilities in the same CVE on a device, the open and closed vulnerabilities are not tracked.	No workaround currently exists.
ITSRM-2992	Tickets can become inconsistent with Issues Counts if the workflows fail due to a cluster being down. Issues will still be captured into a Ticket, but it may result in duplicate Tickets with an invalid count.	No workaround currently exists.
ITSRM-2441	After configuring Archer GRC, Nessus, and/or Rapid7 endpoints, jobs have failed.	The DC service has to be restarted before running any of the workflows or the job will fail when launched.
ITSRM-3494	Rapid7 connection does not work with proxy that needs authentication.	Rapid7 connection will work with no proxy or with a proxy that does not require authentication.
ITSRM-3490	Archer endpoint creation fails when an "&" exists in the user password.	Passwords cannot contain special characters other than "!"

Documentation Errata

This section includes corrections to the RSA Vulnerability Risk Management 1.1 SP1 document set.

Troubleshooting

Note: This is an update to an existing troubleshooting entry in the *RSA Vulnerability Risk Management 1.1 SP1 Installation and Configuration Guide*.

Problem	Description	Remediation
A pop-up error message in MapR UI appears when selecting a single node: RPC to execute 'DISK_LIST' on node:XXX.YYY.ZZZ returned no Data.	In the previous MapR version, the disk information was obtained using SSH. In current version, v3.1 sends an RPC on port 1111 to hoststat on the remote node to execute the desired disk command, DISK_ LIST.	Add Port 1111 on every node where you see the error message as follows: 1. Open vi /etc/sysconfig/iptables. 2. Add the following line: A INPUT -p tcp -m state --state NEW -m tcp --dport 1111 –j ACCEPT 3. Restart service to apply changes service iptables restart.

Documentation Supplement

This section includes additions to the RSA Vulnerability Risk Management 1.1 SP1 document set.

Add the Tenable Nessus v6 Endpoint

For more information, refer to the RSA VRM Installation and Configuration guide.

Procedure

1. Open Connection Manager:
   a. Open a command prompt.
   b. Enter:

   ```
   runConnectionManager.bat
   ```
2. Enter the number for Add Endpoint.
3. Enter the endpoint name.
4. Enter the Nessus v6 Endpoint URL.
5. Enter the Nessus v6 user name.
6. Enter and confirm the Nessus v6 password.
7. Enter the number of days of historical scans to load on the first run.

   Note: The default is 30 days.
8. If you enter True to pull from a file share instead of Tenable Nessus API, complete the following fields:

Field	Description
Authentication type	To run the scan workflow from files on the local machine, enter LOCAL. If the scan file is on a remote machine, enter REMOTE.
File share path	The file share path of the local or remote machine.
File share host name	Host name of the file share. If using remote file share, enter the hostname or IP address of the remote machine.
File share domain	If using remote file share, enter the domain name of the file share.

Field	Description
File share user name	If using remote file share, enter the username credentials to access the remote machine.
File share user password	If using remote file share, enter the password credentials to access the remote machine.

9. If you enter True for Proxy required, do the following:
   a. Enter the proxy host.
   b. Enter the proxy port.
   c. If authentication is required for connection to the proxy, do the following:
      i. Enter the username.
      ii. Enter and confirm the password.

   Note: To configure the Tenable Nessus v6 endpoint through proxy, you must manually copy the Tenable Nessus v6 certificates to the VRM keystore.

10. Once the endpoint is added, enable the scan reports and vulnerabilities.

Enable Scan Reports and Vulnerabilities for Tenable Nessus v6

Procedure

1. Open Connection Manager, as follows:
   a. Open a command prompt.
   b. Enter:

   ```
   runConnectionManager.bat
   ```

2. Enter the number for Edit Endpoint Job Schedules.
3. Enter the number for Edit Workflow Schedules for Nessus v6.x :n6-<*your endpoint name*>.
4. Complete the following fields:

Field	Description
Cron schedule for job getNessusVulns	Provide the cron expression to schedule the getNessusVulns job. If enabled, it is scheduled to run at 22:10 everydayby default.

Field	Description
Set state for job (ENABLE/DISABLE) getNessusVulns	The getNessusVulns job is disabled by default. To run the job, enter ENABLE.
Cron schedule for job getNessusScans	Provide the cron expression to schedule the getNessusScans. If enabled, it is scheduled to run at 0:30 every day, by default.
Set state for job (ENABLE/DISABLE) getNessusScans	The getNessusScans job is disabled by default. To run the job, enter ENABLE.