RSA Vulnerability Risk Management 1.1 SP1

Practitioner Guide

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

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") 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.rsa.com/legal/trademarks_list.pdf**.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 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

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

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.

December 2014

Contents

Preface

About This Guide

This guide contains information to help security analysts and CISOs understand and start working with RSA® Vulnerability Risk Management. It is designed to be used with the RSA Vulnerability Analytics Help and RSA® Archer® GRC Platform Help and documentation.

RSA Archer Documentation

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

Documentation	Location
Platform	On the RSA Archer Community at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**
Solutions, Applications, and Content	On Content tab on the RSA Archer Exchange at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**

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

Guide	Description
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.
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/**.

Support and Service

Customer Support Information	**http://www.emc.com/support/rsa/contact/phone-numbers.htm**
Customer Support Email	**archersupport@rsa.com**
RSA Archer Community	**https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**
RSA Archer Exchange	**https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**
RSA SecurCare® Online	**https://knowledge.rsasecurity.com**

RSA Security Analytics Community	**https://community.emc.com/community/connect/rsaxchange/netwitness**
RSA Download Central	**https://download.rsasecurity.com**

The Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer product roadmap.

The Exchange is an online marketplace dedicated to supporting GRC initiatives. The Exchange brings together on-demand applications along with service, content, and integration providers to fuel the success of RSA Archer clients.

RSA SecurCare Online offers a knowledge base that contains answers to common questions and solutions to known problems. SecurCare Online also offers information on new releases, important technical news, and software downloads.

Chapter 1: Importance and Challenges of Vulnerability Risk Management

Vulnerability Risk Management

In the last few years, the information security industry has seen an upheaval in the understanding and definition of threat management. A string of high visibility, high impact data breaches has clearly defined a turning point in the world of information security.

Multiple studies and reports have been issued on the changing threat landscape. Hactivism, APTs, the digital underground, and many other trends have stressed to companies that threat management, while a core part of information security for years, is not a stagnant science but a continually evolving art. The ability of an organization to manage threats is now paramount to its success as a business and, in some respects, necessary for its survival.

For an IT security organization to protect a company against today's threats, processes, tools, procedures and enablers must be implemented to create a holistic strategy. The program should have a continuous cycle that flows from prevention to detection to response with a feedback loop to ensure that threats are proactively managed as much as possible. While no organization can prevent every threat or patch every vulnerability, the goal should be to identify and prevent as much as possible, effectively detect and respond to active threats, learn from events and incidents, and improve going forward. A key part of this strategy is vulnerability management.

The objectives of a vulnerability management program are to:

- Effectively and efficiently identify vulnerabilities within an organization
- Remediate vulnerabilities where threats can cause the most impact to the organization

Organizations face multiple challenges when it comes to vulnerability risk management:

- The lack of business context prevents fast prioritization and efficient response to possible threats to the infrastructure.

- Companies are identifying possible threats through disconnected processes and have difficulties merging those activities into one consistent view of threats to the organization.
- Proactive measures such as vulnerability scanning create massive amounts of data but lack the business context needed to prioritize work, so IT teams are directed to fix everything and struggle to keep up. Additionally, with little connection to configuration management processes, the company sees vulnerabilities over and over because the root causes – patching and secure configurations – are disconnected from proactive vulnerability processes.

Challenges in Vulnerability Risk Management

Several key challenges make vulnerability risk management tools and processes difficult for an organization to acquire, develop, and use with ongoing confidence and success.

Common Asset Identifier

Companies have many repositories of assets. The RSA Archer Enterprise Management solution offers a system to store asset data. Vulnerability scanners have their own internal repositories of assets identified during scanning. Companies also have internal CMDBs and other asset repositories that catalog IT assets. Companies usually are then lacking one unifying descriptor or identification tag for an asset.

A key challenge for vulnerability management is to connect these systems with a common asset identifier. When vulnerabilities are found on a device, the device might be known to the organization and be part of some asset repository. Vulnerabilities on these devices represent a significant portion of the security risk in an organization.

In addition, unknown devices may be found during a vulnerability scan. These devices also represent risk to the organization and need to be incorporated into the overall threat view.

Large Number of Assets

Many companies want to increase their coverage of vulnerability management beyond bounded compliance scopes to all types of devices. Vulnerability scanners are easily expanded – many just require a range of IP addresses – and can identify and report on vulnerabilities on large amounts of devices. However, this expansion of scope must also be addressed on the process, reporting and prioritization fronts.

The expansion of vulnerability scanning beyond small compliance oriented programs allows an organization to identify potential vulnerable systems that can be used to compromise data, launch lateral attacks across the organization, or provide footholds for long term advanced data breaches. If the company is not prepared to manage the larger number of assets within the vulnerability management program, the flood of asset information will make remediation efforts increasingly difficult.

Therefore the vulnerability management strategy must account for an increasing asset scope, but within a framework that addresses critical assets first.

Large Number of Vulnerabilities

Vulnerability scanners create a large amount of data. Each scan may find tens and potentially hundreds of thousands of vulnerabilities on a single device. Vulnerabilities can range from severe (for example, active exploits) to informational (for example, general system profiling).

Companies can run the scans on a regular basis, creating a large and ever-growing data set. Additionally, some companies need to retain this information for compliance purposes for a set retention period which can extend to seven years or more.

Constant Stream of Vulnerabilities

Vulnerabilities are identified and published on a daily basis. Threat intelligence feeds help companies keep track of new and changing vulnerabilities. However, as the desire is to connect the incoming threat feed information with the data coming from vulnerability scanners, the need to synchronize vulnerability data is a significant challenge.

Companies want to connect their internal analysis of vulnerabilities with external perspectives and then have that internal analysis affect the vulnerability scan results. For example, a threat feed may identify a vulnerability as High criticality. However the company, after analysis, may upgrade or downgrade that criticality based on business requirements, and may want their criticality applied instead of the scanner's criticality when the vulnerability is found again.

Remediation and Exceptions

The main goal of the vulnerability management program is to reduce attack vectors through remediation of vulnerabilities. This can be achieved through various means, such as patching, configuration changes, and detective controls. From a vulnerability scan perspective, once a vulnerability is found on a device, an administrator must fix the vulnerability. In some cases, this is possible through remediation. In other cases, vulnerabilities cannot be patched and must be granted an exception from remediation using business review and approval processes.

Remediation processes require an ongoing picture of the efforts to patch or eliminate vulnerabilities. This requires administrators to identify which vulnerabilities on which devices are to be patched.

Exception processes require a workflow in which the administrator requests an exception and the exception is approved and granted. This requires administrators to identify which vulnerabilities on which devices require an exception. After an exception is granted, the next time that the vulnerability scanner finds that specific vulnerability on the designated device, the vulnerability should be tagged as already granted an exception and requiring no further work. Most exceptions are granted for a limited period of time, so exception processes must also have ways to manage what happens when an exception expires.

The objective of the vulnerability management program is to know which vulnerabilities on which devices must be fixed and which are granted an exception and require no corrective action. This allows the company to see the actual state of the vulnerabilities on devices:

- Active but no action yet defined
- Active and flagged for remediation
- Active and flagged for exception

Visibility into the current state of device asset vulnerability is of high business value for the organization and is a key challenge of the solution given the number of possible devices and vulnerabilities.

Business Needs for Vulnerability Risk Management

Vulnerability risk management must include governance that clearly establishes who is responsible for specific IT security risks. Processes must be optimized with appropriate workflow to ensure that resources are being used as efficiently as possible. In addition, vulnerability risk management needs a high level of visibility and analytics to determine the current state of security threats. Finally, all companies want to deploy intelligent controls that make sense for the business, are cost effective, and can evolve with the organization.

Too many times, companies in the past implemented controls for control's sake, often using a point technology solution or an inefficient manual process, simply to satisfy the regulator or auditor. This can no longer be the case. Companies now want controls to be rationalized, harmonized, and efficient so that they are highly auditable but flexible to adjust to new risk and changing environments.

Chapter 2: Introduction to RSA Vulnerability Risk Management

RSA Vulnerability Risk Management

RSA Vulnerability Risk Management (RSA VRM) takes a Big Data approach to helping security teams identify and prioritize high-risk threats. Built on the RSA Archer platform, RSA VRM helps organizations proactively manage IT security risks by combining asset business context, actionable threat intelligence, vulnerability assessment results, and comprehensive workflows.

Benefits of RSA Vulnerability Risk Managment

RSA Vulnerability Risk Management is designed to support the business needs for vulnerability risk management. It supports governance, visibility, analytics, and intelligent controls that are highly auditable and flexible.

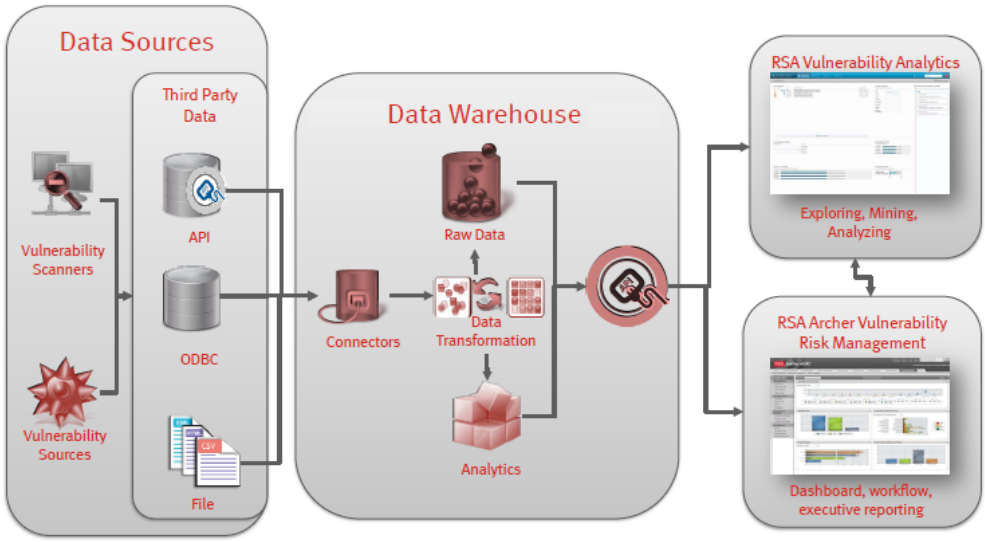
Key capabilities of RSA VRM include:

- Leveraging Big Data analytics to aggregate massive amounts of security data.
- Creating and maintaining an accurate asset catalog.
- Prioritizing and classifying issues based on business context, threat intelligence, and vulnerability scan results.
- Tracking issues over the entire lifecycle – detection, remediation, and verification.
- Managing issues, exceptions, and remediation workflows.
- Assign, measure and report on vulnerability program KPIs.

High-Level Architecture of RSA Vulnerability Risk Management

The following illustration is a logical view of the technical architecture of RSA Vulnerability Risk Management. The architecture is comprised of four major elements:

- Data Sources
- RSA Analytics Warehouse (MapR)
- RSA Vulnerability Analytics
- RSA Archer Vulnerability Risk Management



Data Sources

API-based, file-based (.csv or .xml), and ODBC-based data sources provide the device asset and threat information that RSA Vulnerability Risk Management (RSA VRM) requires to work. RSA VRM pulls data from configured data sources daily at midnight, ensuring that asset and threat information in RSA VRM is updated with the latest device and known vulnerability knowledge.

Third Party Device and Vulnerability Data

RSA VRM supports these sources of vulnerability scanner data:

- McAfee Vulnerability Manager
- QualysGuard Vulnerability Management
- Rapid7
- Tenable Nessus

RSA VRM supports the National Vulnerability Database for common vulnerabilities and exposures.

Device and Business Context Data from RSA Archer

RSA Archer applications are the primary data source for the business context of device assets. They can contribute device information such as administrator, owner, manager, business unit, and facility to the device data gathered by scanners.

In addition, devices discovered by a vulnerability scan can be pushed to RSA Archer, where business context can be added. Bi-directional data synchronization allows RSA VRM to feed device information into RSA Archer and RSA Archer to provide the business context for discovered devices to RSA VRM.

Device and Business Context Data from CSV and XML Files

Organizations with information about device assets and business context stored in miscellaneous applications and files can get the data into RSA VRM by moving it into a .csv-formatted or .xml-formatted file, and then importing the file.

RSA Analytics Warehouse (MapR)

The RSA Analytics Warehouse (MapR) consumes all of the data coming in from data sources. It standardizes and aggregates the content from the disparate sources and provides fast access to the whole body of information.

The warehouse is designed to store and manage big data volumes of content, including detailed information about:

- Thousands to tens of thousands of devices and vulnerabilities.
- Millions of vulnerability scan results that RSA Vulnerability Analytics generates using the device and vulnerability data.

RSA Vulnerability Analytics

The RSA Vulnerability Analytics (RSA VA) part of RSA VRM analyzes the aggregation of data in the RSA Analytics Warehouse (MapR) to discover and prioritize vulnerability issues for device assets.

The RSA VA interface gives security analysts a way to view and explore discovered issues and the aggregated data behind them. Analysts can filter data into logical and manageable content groups using its search and query feature. They can find out quickly about new or high-severity vulnerabilities that may impact infrastructure security by defining rules that generate alerts when these situations arise.

RSA Archer Vulnerability Risk Management Solution

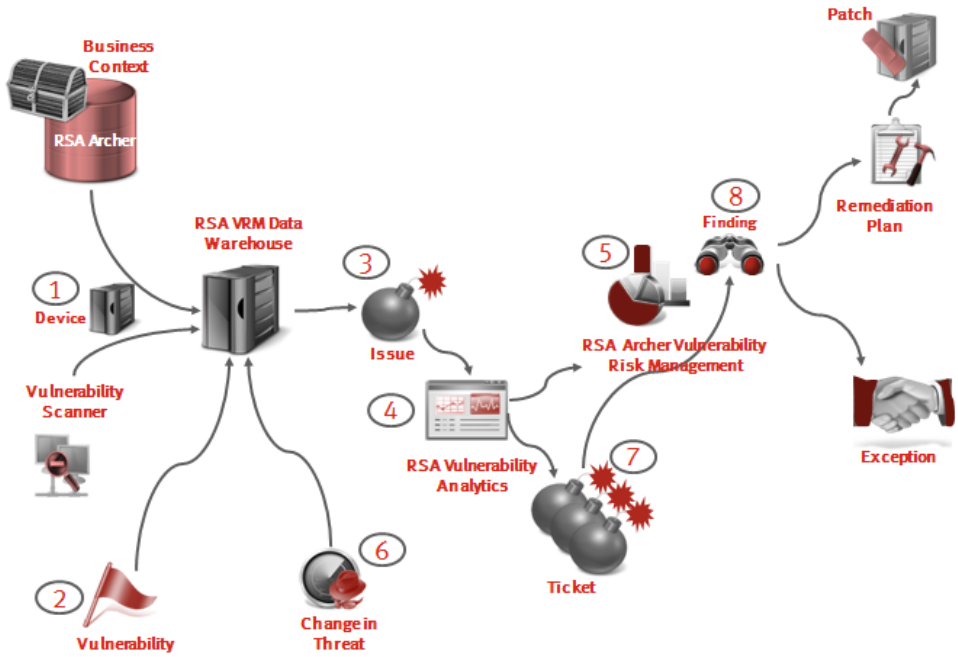
The RSA Archer Vulnerability Risk Management (RSA Archer VRM) solution provides GRC capabilities that enable automation of controlled business processes around vulnerability metrics and issue remediation.

RSA Archer VRM provides the automated workflow, dashboard, and reporting capabilities that security and IT teams need to remediate issues and review and approve remediation plans and exception requests. In addition, the solution provides visibility into the performance of the vulnerability management program to security management through the capture of key metrics.

RSA Vulnerability Risk Management Workflow

The RSA Vulnerability Risk Management solution is designed to streamline the process of identifying vulnerable devices in the infrastructure, prioritize issues based on business criticality, vulnerability attributes, and emerging threat intelligence, and track remediation efforts related to the vulnerability.

The basic workflow is as follows:



1. Devices in the infrastructure are cataloged or discovered, and business context such as use of device and criticality is added to the device catalog stored in the RSA Analytics Warehouse (MapR). RSA Vulnerability Risk Management (RSA VRM) analyzes, normalizes, and organizes all of this data to provide a clear understanding of the nature, usage and value of IT assets.
   a. Vulnerability scanners identify devices within the infrastructure. The method of discovery varies but the end result is a catalog of devices known or identified by the scanner. Vulnerability scanners also scan and test devices. All scan data is imported into the RSA Analytics Warehouse (MapR).
   b. The RSA Archer Enterprise Management solution can provide business context information about devices in the infrastructure. IT and security organizations can catalog devices and provide attributes for known devices such as asset owner, business criticality, and other metadata that defines the use and value of the device within the business.
2. Vulnerabilities are tracked in a central catalog stored in the RSA Analytics Warehouse (MapR) and viewable in RSA VA. Information about vulnerabilities

can come from the individual scanners or from an external source such as the National Vulnerability Database (NVD). IT and security administrators use the vulnerability information such as the type of vulnerability, the potential threat, the affected software, and other metadata to understand the technical impact of the vulnerability.

3. All device and scan data in the RSA Analytics Warehouse (MapR) is aggregated and normalized for computational use by RSA Vulnerability Analytics (RSA VA). An issue is created when RSA VA finds an individual vulnerability on a specific device.
4. RSA VA enables IT administrators to track, search, and generate reports on scan results to identify critical issues.
5. RSA VA sends metrics for key performance indicators (KPIs) for issue tracking and discovery and resolution trends to the RSA Archer Vulnerability Risk Management solution (RSA Archer VRM) for management reporting. This gives the security management team visibility into risks in the infrastructure.
6. Vulnerabilities can change threat levels, such as exploit code for a vulnerability being published or an active exploit attacks being executed. Automatic periodic updates to vulnerability information are collected in the RSA Archer Platform and viewable in RSA VA to give security administrators late-breaking information about vulnerability changes and emerging threats.
7. Issues identified as very critical can be bundled into an RSA VA ticket and sent to RSA Archer VRM, where the ticket becomes a Finding for tracking and resolution. Issues can be critical for a variety of reasons:
    a. The vulnerability profile changed (for example, exploit code published or active exploit attacks are known) and the potential threat posed by systems vulnerable to the attack is higher.
    b. The devices involved have high value to the business and the security or IT team wants to ensure a quicker patching cycle than the normal cycle.
    c. The vulnerability was not patched as part of the normal cycle due to some patch issue (machine was not rebooted properly, the configuration change was not applied correctly, and so on), so the issue needs to be escalated.
8. Findings in RSA Archer VRM are managed through either an exception request process because the issue cannot be resolved and an exception must be approved, or a remediation plan process where the issue will be part of an effort to resolve. Findings can then be tracked and reported in RSA Archer VRM. Changes in Finding status in RSA Archer VRM are automatically sent to RSA VA, ensuring that issue progress is the same in both interfaces.

Chapter 3: Implementation Lifecycle

Introduction

A successful deployment of RSA Vulnerability Risk Management requires identifying data sources, installing RSA VRM components and connecting them to the data sources, and reviewing incoming data and engaging with stakeholders to define and refine business rules and processes implemented with RSA VRM.

Deploy RSA Vulnerability Risk Management

Complete the following procedures to deploy and improve RSA Vulnerability Risk Management.

Procedure

1. Identifying the Data Sources to Import into RSA VRM
2. Deploying RSA VRM Components
3. Importing Data from Data Sources into RSA VRM
4. Defining and Implementing Your Business Rules and Processes
5. Refining Your Business Rules and Processes

Identifying the Data Sources to Import into RSA VRM

Defining the data to import into RSA VRM is critical to a successful deployment. The accuracy and completeness of issues discovered by RSA VRM is only as good as the source data it contains.

Investigate the sources of device data that you will use in RSA VRM from throughout your enterprise. Find out both the location of the data sources and how to get data out of the sources and into RSA VRM. If a data source is not under your control, you will have to request credentials to access it from owning organizations.

Making time early to define, get access to, and verify your access to data sources makes RSA VRM deployment as fast and straightforward as it can be.

Vulnerability Data

The data feed that pulls vulnerability data from the National Vulnerability Database (NVD) is built into the RSA VA component of RSA VRM. These feeds become active after installation and continuously update known vulnerability information in RSA VA. Vulnerability Data can also be pulled from scanners that provide the data.

Device Asset Data from Scanners

Vulnerability scanners automate the gathering of device asset data from throughout your enterprise. Supported scanners include:

- McAfee Vulnerability Manager
- QualysGuard Vulnerability Management
- Rapid7
- Tenable Nessus

To get device data from scanners into RSA VRM, you set up data feeds from the scanners to RSA VA. RSA VA needs the location of the scanner and credentials to copy the required data from the scanner.

Device Asset Data Available in CSV Format

Some device asset data in your organization may be stored in files or spreadsheets or in products other than supported scanners. To use data from these sources in RSA VA, output or convert the data into a .csv-formatted file. If the data is changed regularly, you can implement a .csv-based data feed from the source into RSA VA to get updates.

Device Asset Data Available in XML Format

Generic scanners often store device asset data in XML format. You can import this stored XML data into RSA VA by setting up and endpoint in the RSA VA Connection Manager.

Device Asset Data for Business Context from RSA Archer

Vulnerability risk assessments can be prioritized better if the business context of a device is part of the assessment. You can add this context to device information by pulling in device data from RSA Archer applications that include device details such as owner, manager, business unit, and facility.

To get device data from RSA Archer into RSA VRM, you must synchronize data from the Devices application in the RSA Archer Enterprise Management solution with RSA VA. This requires credentials for the applications and content. RSA VA merges the device data from scanners and RSA Archer applications so that all device information becomes available in both RSA VRM and RSA Archer.

Deploying RSA VRM Components

Deploying RSA VRM involves installing, configuring, and connecting these components:

- RSA Analytics Warehouse (MapR) as the data storage and manager for all RSA VRM content.
- RSA Vulnerability Analytics as a standalone Web application on a secure machine.
- The RSA Archer Vulnerability Risk Management solution on an RSA Archer instance.

For instructions on how to install and configure software components of RSA VRM, see the *RSA Vulnerability Risk Management Installation and Configuration Guide*.

Importing Data from Data Sources into RSA VRM

Pulling existing data into RSA VRM gives you a good starting point for developing business rules and processes that you can automate using the product. You pull all data into the RSA VA component of RSA VRM, where it is standardized and aggregated in preparation for analysis.

For instructions for loading data from the data sources you defined earlier, see the *RSA Vulnerability Risk Management Installation and Configuration Guide*. You need the locations of and credentials for the data sources to set up and activate the flow of data into RSA VA.

Data Source	How to Import Source Data into RSA VA
Vulnerability data	The vulnerability data feed into RSA VA from the National Vulnerability Database (NVD) is built-in and becomes active after installation.
Device asset data from scanners	Using RSA VA, set up a data feed from the scanner to RSA VA using the target location and the credentials required to access the data.
Device asset data from files, spreadsheets, and other applications	Convert the data to a .csv or .xml file and use RSA VA to import the .csv or .xml file. **Important:** If you are using a .csv file, format the file with column names using the field names found in the original XML file.
Device asset data from RSA Archer	During installation, set up a connection to the RSA Archer instance that includes the Devices application containing the data, using credentials sufficient to access and update the data.

Defining and Implementing Your Business Rules and Processes

There are two critical parts to defining business rules and processes for RSA VRM:

- Reviewing data in RSA VA.
- Engaging stakeholders responsible for issue remediation.

Reviewing Data in RSA Vulnerability Analytics

After the initial data loads into RSA Vulnerability Analytics, security analysts can perform an initial vulnerability analysis to identify trends, weak points, and missing coverage in current vulnerability discovery and issue management across device assets.

As the initial analysis of data progresses in RSA VA and as the business processes become defined, security analysts can begin to write the rules in RSA VA that automate issue handling and to assign users of the RSA Archer Vulnerability Risk Management solution to participate in remediation planning and exception request approvals.

The following table describes some of the types of rules and processes that security analysts can define in RSA VRM to automate the handling of asset information and issues. Other use cases become apparent as you analyze incoming vulnerability and device data. The RSA VA rules engine can be used to quickly build alerts for different types of vulnerability scenarios.

Type of Rule or Process	Description
Critical asset handling	Rules that factor in both the severity of a found vulnerability and the business value of a device can prioritize alerts by the business value of devices. Having the business context of a device enables intelligent and timely allocation of work towards the most business-critical device assets.
Asset identification handling	Scanners feeding into RSA VA may find devices that are not in RSA Archer. Rules can route discovered asset information into RSA Archer, where notifications can be triggered for review or completion of the device information that is in turn sent back to RSA VA.
High-impact vulnerability routing	Rules can recognize when a vulnerability may severely impact devices that drive critical business operations and can escalate issue investigation and remediation on faster timetables than enabled by routine issue-handling rules.
High-risk issues handling	Rules set up to detect a serious vulnerability may affect critical device assets can escalate investigation and remediation to more quickly protect the assets.

Type of Rule or Process	Description
Ticket creation and escalation	The business or industry may require that certain types of issues be escalated to go through more formal and visible remediation plan and exception request processes. Rules in RSA VA can bundle issues into tickets and send them to the RSA Archer Vulnerability Risk Management solution, where they become findings. The solution can be set up to drive the findings through the required remediation and exception processes. Progress on a finding is automatically transmitted to the RSA VA ticket to close the information loop.

For instructions on how to write rules in RSA VA, see the RSA Vulnerability Analytics Help.

To see the rules defined by default in RSA VA, check the Rules list (Administration > Rules) for System rules in the RSA Vulnerability Analytics interface.

Engaging Stakeholders Responsible for Issue Remediation

Security analysts and CISOs must engage other stakeholders to define remediation processes and role ownership. A combined team of security and stakeholder personnel should work together to define the types of vulnerability issues important to the organizations they support and the business criticality of device assets owned by the organizations. This team must also define the business processes and role owners for remediation of issues.

These definitions and agreements provide details that can be used to implement rules in RSA Vulnerability Analytics and define remediation and exception processes in the RSA Archer Vulnerability Risk Management solution.

To see the roles involved in remediation and exception processes, see the remediation and exception request interface pages that are part of the RSA Archer Vulnerability Risk Management solution. For instructions on how to assign users to remediation and exception approval roles defined in the solution, see the RSA Archer Platform Help Center.

Refining Your Business Rules and Processes

The initial implementation of rules and processes should transform over time into a continuous RSA VRM improvement loop. Security analysts and CISOs can look at accumulated vulnerability discovery and remediation information in different ways to find areas where vulnerability risk management is working smoothly, and to find weak areas that can be strengthened by expanding or modifying RSA VRM.

Ongoing improvements to data in RSA VRM depend in large part on the needs and requirements of the business, which change over time. Because stakeholders outside of the security team best understand the changing needs and requirements of their business units, it is critical that the security team continue to inform them about and engage them in defining improvements and changes to RSA VRM.

Improvements can take many approaches, including:

- Fine-tuning existing RSA VA rules to improve efficiency or more logically group issues into tickets.
- Creating new RSA VA rules to handle more and different types of data.
- Adding new sources of data, such as data feeds from more vulnerability scanners.
- Redefining business processes and assignments to streamline issue remediation and the approval process for issue exceptions in the RSA Archer Vulnerability Risk Management solution.

The important point to consider is that vulnerability risk management should be an evolving program within the security strategy. As RSA VRM provides insight into the overall program, security and IT teams can partner with the business to continually improve the process. Vulnerability management can then transform from a "check the box" compliance exercise to a process that reduces overall security risk and protects critical business assets.

Chapter 4: RSA Vulnerability Analytics

Components of RSA Vulnerability Analytics

The following table briefly defines the primary components of RSA Vulnerability Analytics (RSA VA).

Component	Definition
Alert	A notification to the security analyst that a rule matched a set of issues. The notification appears in the Unread Alerts chart in the RSA VA Dashboard.
Device	A collection of information about a single device asset. It includes device details such as IP address, device owner and manager, and business criticality. Sources of device information are scanners and the Devices application in RSA Archer. **Note:** When a device is first imported into RSA VA, the device is in an Unmatched state. You can set it as a Matched device within RSA VA.
Issue	One instance of a vulnerability found on one device. RSA VA compares device information to known vulnerabilities and creates an issue for each found vulnerability on a device.
Rule	Search criteria that finds issues with specific characteristics, actions to take when the issues are found, and a schedule that runs the search at specified intervals to find issues matching the characteristics. Actions can include creating an alert that includes the issues, sending email notifications about the issues, bundling the issues into a ticket, and changing the properties of the Vulnerabilities, Devices, or Issues.
Ticket	A set of issues that are related in some way, such as all issues

Component	Definition
	occurring on a single device or all issues found on device groups owned or managed by a specific IT team.
Vulnerability	A set of information about a known weakness in hardware or software that may allow an attacker to gain access to data or control the machine. It includes a name and description of the vulnerability, a severity rating, and recommendations for remediation. Sources of vulnerability information are publicly available vulnerability databases.

Working Daily with the Dashboard

The Dashboard is the opening view for the security analyst in RSA Vulnerability Analytics. Its charts summarize everything going on in RSA VRM and provide the daily starting points for your vulnerability management work.

The Dashboard gives you fast entry into these tasks:

- Reviewing and acting on alerts (**Unread Alerts** chart)
- Verifying RSA VA operational status (**Vulnerability Analytics Timeline**)
- Monitoring issue status changes (**Issues By Status** chart)
- Monitoring detection and remediation velocity (**Issue Response Time** and **Remediation Time** charts)
- Correcting problems with fixes that break **(Inadequate Fixes** chart)
- Confirming that devices are scanned **(Scanner Coverage** chart)

Unread Alerts Chart

The Unread Alerts chart is your immediate daily work list. It lists all alerts that you need to review and take action on. You review an alert by clicking its Count or Triggered Rule to open and explore searchable and sortable details.

RSA Vulnerability Analytics Timeline

The Vulnerability Analytics Timeline is your chronological view of all activity in RSA VA. Review the information listed in the timeline daily to ensure that RSA VA is operating as you expect.

You can quickly see when RSA VA operations ran or updated content, and if operations completed successful or not. Red icons highlight unsuccessful operations that may be problems you need to investigate and resolve.

Issues by Status Chart

The Issues By Status chart shows if issue counts by status are increasing and decreasing over time as you expect. Look at this chart periodically to check for increases or drops in issue counts that suggest unexpected activity.

You can explore the data behind a point that seems too high or low by clicking it to open searchable and sortable details for the issues in the state at that time.

Issues Response Time Chart

The Issue Response Time chart summarizes how quickly issues were found and remediated over the past three months. Check this chart periodically to confirm that issue remediation, detection rates, and the average issue age meet your business requirements.

If a point is outside an acceptable range, you can click it to open and explore searchable and sortable details for reasons the numbers appear unacceptable and ideas about how to improve response time.

Remediation Time Chart

Use the Remediation Time chart to monitor the velocity of issue resolution and compare it against your business requirements.

The dark bars on the chart represent the percentage of issues resolved within 14, 30, 90, and 180 days of their discovery. You see the percentage number when the cursor hovers over the small bar.

A short bar indicates a high percentage of unresolved issues, which suggests that issues are not being resolved in a timely fashion. You can click a bar to open and explore searchable and sortable details for ideas about how to improve remediation time.

Inadequate Fixes Chart

The Inadequate Fixes chart displays the set of fixed issues that revert to an unfixed state. Review this chart and its issue details periodically to look for reasons the fixes failed and get ideas about how to improve rules and processes so that similar inadequate fixes are avoided.

The dark bars on the chart represent the percentage of reopened issues over that time. You see the number of reopened issues when the cursor hovers over the small bar. You can click a bar to open and explore searchable and sortable issue details.

Personnel who remediate issues move them manually to a fixed state after finishing remediation work. Issues that move from fixed to reopened suggest that your remediation process has flaws that require investigation and correction.

Issues are moved to a verified state automatically when a later scan cannot find a vulnerability found on a device by a previous scan. Issues that move from verified to reopened require investigation because they can imply any of several conditions, such as:

- Your scanners are reporting vulnerabilities incorrectly.
- Detection capabilities of your scanners are improving over time.
- Your usage of the scanner is getting better over time.

Scanner Coverage Chart

Checking the Scanner Coverage chart daily helps you make sure that devices are being scanned for vulnerabilities successfully on defined schedules.

The dark bars on the chart represent the percentage of devices scanned within the past 14, 30, 90, and 180 days. You see the percentage number when the cursor hovers over the small bar.

A short bar indicates a high percentage of unscanned devices, which may suggest problems such as broken connections between the scanner and devices and scans not running or completing as scheduled. You can click a bar to open and explore searchable and sortable details to figure out what caused the scan problems and ways to correct them

Exploring Data in Reports

Reports give security analysts a simple yet powerful way of interactively exploring the data stored in RSA VA. They provide views of the key performance indicators (KPIs) that flow from RSA VA into RSA Archer. The Reports interface is your print preview window, allowing you to review KPIs before RSA VA pushes them to RSA Archer for review by the CISO and teams that participate in remediation processes.

As historical and new asset data is aggregated and normalized, the reports give you more understanding about and insights into the state of vulnerability risks across your enterprise. The summary charts on the Dashboard connect to these reports to let you see and explore details.

You use the interactive charting options to sort and filter report data by a combination of date range and data dimensions. The dimensions available for filtering depend on their relevance to the report and may include details such as issue status, device group, business unit, and CVSS score.

Because RSA VA includes more data and dimensions than the RSA Archer Vulnerability Risk Management solution, you can use RSA VA to do more accurate device grouping according to IT responsibilities based on business unit, operating system, and other data dimensions. Fine-tuning device groups through RSA VA allows you to create reports that exactly match asset sets to the IT personnel and teams responsible for handling specific types of remediation.

Key Performance Indicators in Reports

You can review many facets of these KPIs using the Report interface of RSA VA:

KPI	Description
Issue State	Number of issues currently in each state status.
Authenticated Scan Coverage	Percentage of known devices scanned successfully during specified time periods, using valid authentication credentials and roles.
Scan Coverage	Percentage of known devices scanned successfully during specified time periods, with and without authentication.
Average Time to Detect	Average time it takes the scanner to find known vulnerabilities on a device after the scanner is started. For vulnerabilities published prior to the first scan of a device, this is measured from the time that the scanning program started doing device scans. For newer vulnerabilities, this is measured from the time that the vulnerability was first publicly known.
Average Issue Age	Average time that issues are open before reaching final resolution. For issues that are still open at the time the report runs, this is the time since the issue was first found. For fixed or verified issues, this is the time it took to fix the issue.
Inadequate Fixes	Count and measure of how often issues are found by the scanner after IT personnel moved them to a fixed state and after the scanner has verified them as fixed.
Remediation Percentage	Percentage of issues that IT personnel fixed within a certain time window, either through an automated process that the scanner can detect or through a remediation workflow driven by the RSA VRM solution.
Average Time to Remediate	Average time it takes IT personnel to remediate known issues, either through an automated process that the scanner can detect or through a remediation workflow driven by the RSA VRM solution.

Drilling into Data with Search

Search is your primary analytical tool for drilling deeply into stored data available to RSA VA. Use it to search hundreds of thousands of stored data records for the data and metrics most important to you, all in real-time.

You can drill down through any stored attribute into any device, vulnerability, and issue record in search results to see more detailed information. The detailed information is always a relevant combination of information collected from scans, RSA Archer, and vulnerability data feeds.

You filter search results to the subset of data you want to see and work with using a query tools on each search page. You can group search results with the simple selection of a data field. To reorganize the data display for your search results, you change which fields are displayed and their sort order using column header dropdowns.

After you filter search results to the data subset you want, you can export the data into a Microsoft Excel file for use outside of RSA VA. The export operation outputs all field labels defined for each item as well as all field values stored for the item.

Device Search

The search feature for devices gives you a complete window into all device information stored for RSA VA use. Use it to monitor asset discovery and organize and synchronize assets with RSA Archer.

Using this page, you can change a data dimension for multiple devices at once by selecting the devices and making an Edit selection. You can also push collected data for multiple selected devices to RSA Archer.

You can select a device in the search results to see all data stored about it.

Vulnerabilities Search

The search feature for vulnerabilities is your window into all of the vulnerability information gathered from configured vulnerability data feed sources.

Using this page, you can change the CVSS overall score of one or more vulnerabilities by selecting them and entering a different score.

Important: Before changing CVSS overall scores, be aware that the scores are imported from public vulnerability sources and summarize expert assessments of vulnerability severity using these standard ranges:

- 0-3.9 is a minor vulnerability.
- 4.0-6.9 is a major vulnerability.
- 7.0-10.0 is a critical vulnerability.

You can select a vulnerability in search results to see all information stored about it.

Issues Search

The search feature for issues is your window into all vulnerabilities found by RSA VA's intelligent analysis of device scan and vulnerability data. Each issue represents one occurrence of one vulnerability on one device asset.

You can select an issue to see all data stored about it. You can also select one or more issues to assign them to IT personnel for investigation, or to change their remediation due date or status.

Queries Search

You create and manage searches using the query feature on the Search page.

You construct search queries using a standard query syntax based on the Apache Lucene query syntax. A query can include any number and combination of stored data attributes. These give you the utmost flexibility in slicing and dicing your data and optimize your ability to organize and analyze the flood of data around vulnerability risk.

In addition to constructing search queries, you can save search queries that you want to run later, manage your saved queries, and create rules that take query results and create an alert for them, send an email notification about them, and change their data attributes. You can also create a ticket for a set of issues compiled by a search query.

Search Query Strings Built into RSA Vulnerability Analytics

RSA VA includes built-in search queries that you can run and look at as models for creating your own query strings.

The following table lists some of the built-in search query strings for device assets.

What the Query Finds	Search Query String
Device added in the last 30 days	first_published_date:[NOW/DAY-30DAY TO NOW/DAY] AND asset_tracking_state:M
Open issues on high criticality devices	asset_criticality:H AND issue_count:[1 TO *] AND asset_ tracking_state:M
Devices with no assigned administrator	-administrator_id:* AND asset_tracking_state:M

The following table lists some of the built-in search query strings for issues.

What the Query Finds	Search Query String
High-severity active issues	cvss_score_severity:HIGH AND (state:ACTIVE OR state:REOPENED) AND device_asset_tracking_state:M
Issues with no assignee	-assignee:* AND (state:ACTIVE OR state:NEW OR state:REOPENED) AND device_asset_tracking_state:M

What the Query Finds	Search Query String
Issues with exceptions expiring in the next 30 days	due_date:[NOW/DAY TO NOW/DAY+30DAY] AND state:EXCEPTED

The following table lists some of the built-in search query strings for vulnerabilities.

What the Query Finds	Search Query String
Vulnerabilities published in the last 7 days	published_date:[NOW/DAY-7DAY TO NOW/DAY]
Remotely exploitable, in-the-wild vulnerabilities	(temporal_exploitability:F OR temporal_exploitability:H) AND (cvss_accessvector:A OR cvss_accessvector:N)
High-severity vulnerabilities (CVSS score > 7.0)	overallscore:[7 TO *]

Automating Data Handling with Rules

Rules are triggers that automate the handling of data that flows into RSA VA.

You create rules to automate different types of operations on search results that meet the search criteria that you specify, such as:

- Create alerts for search results that are new devices discovered by a scan.
- Send email notifications about search results that are newly discovered and highly critical issues.
- Change a data attribute for a collection of search results, such as setting the device criticality to HIGH for devices found to have a web or database listener.
- Create a ticket for issues that require fast attention, such as new issues found to have very high CVSS scores.

Rules in RSA VA are conceptually similar to rules that trigger operations in other applications. Each rule includes a search query to find devices, issues, vulnerabilities, or tickets that match it. A rule also includes a schedule in standard cron format and an action to perform if its search query finds items that match it.

You can apply rules to four types of RSA VA components:

- Devices - For example, you can write a rule to automatically assign a specific user or group to the Administrator attribute for devices with names ending in

RAW.

- Issues - For example, you can write a rule to create an alert for a set of issues with a CVSS score greater than 7 on critical devices.
- Vulnerabilities - For example, you can write a rule to create an alert for newly published vulnerabilities arriving from vulnerability data feeds that have an exploitability setting of Active and no Remediate Level.
- Tickets - For example, you can create an alert for all new tickets found to have a severity of high.

Rules Built Into RSA Vulnerability Analytics

RSA VA includes built-in rules scheduled to run periodically by default. You can use these rules as models for creating your own rules to automate actions that drive your business processes. For instructions on how to create a rule, see the RSA Vulnerability Analytics Help.

The following table lists the search query string and actions defined in some of the built-in rules that act on device assets.

Rule Name	Description of Actions Triggered	Search Query String
Device with open web and database ports	Sets the criticality to HIGH for any system with both a web and database listener. This includes ports 80, 443, 1433 (MSSQL), 1521 (Oracle), 3306 (MySQL), and 5432 (PostgreSQL)	(network_services_list:tcp-80 OR network_services_list:tcp-443) AND (network_services_list:tcp-1433 OR network_services_list:tcp-1521 OR network_services_list:tcp-3306 OR network_services_list:tcp-5432) AND asset_tracking_state:M
Device added in last 30 days	Creates an alert and launches the Archer Device workflow for any device added to RSA VRM in the last 30 days	first_published_date:[NOW/DAY-30DAY TO NOW/DAY] AND asset_tracking_state:M

The following table lists the search query string and actions defined in some of the built-in rules that act on issues.

Rule Name	Description of Actions Triggered	Search Query String
Issues overdue by 7 days	Creates and opens a ticket for any issues that are more than a week past their due date	due_date:[* TO NOW/DAY-7DAY] AND (state:ACTIVE OR state:NEW OR state:REOPENED) AND device_asset_tracking_state:M

Rule Name	Description of Actions Triggered	Search Query String
Expired Exceptions	Creates an alert when there are any expired issues and sets their state back to ACTIVE	due_date:[* TO NOW/DAY] AND state:EXCEPTED

The following table lists the search query string and actions defined in a built-in rule that acts on vulnerabilities.

Rule Name	Description of Actions Triggered	Search Query String
Remotely exploitable, in-the-wild vulnerabilities	Creates an alert whenever remotely and easily exploitable vulnerabilities are published or updated (CVSS Temporal Exploitability vector =F [unctional] or H[igh] , CVSS Base Access Vector = [A] djacent Network or [N] etwork)	(temporal_exploitability:F OR temporal_exploitability:H) AND (cvss_ accessvector:A OR cvss_ accessvector:N)

The following table lists the search query strings and actions defined in some of the built-in rules that act on tickets.

Rule Name	Description of Actions Triggered	Search Query String
Tickets overdue by 7 days	Creates an alert for any tickets that are more than a week past their due date	due_date:[* TO NOW/DAY-7DAY] AND state:ACTIVE
Tickets with more than 100 issues	Creates an alert for any tickets that have more than 100 issues assigned to them	issue_count:[100 TO *] AND state:ACTIVE

Remediating Groups of Issues as Tickets

Tickets are the connection between RSA Vulnerability Analytics and the RSA Archer Vulnerability Risk Management solution. You create tickets to move groups of issues into RSA Archer, where they appear as Findings that flow into the remediation business process.

A ticket is a rule-created or manually-created set of issues. Only issues in the New, Active or Reopened states can be bundled as a ticket. If the query in the results include any other issue state, they do not show up in the ticket. To automate ticket creation, you can create an issue rule that creates a ticket as one of its actions. When the rule finds issues, it bundles them into a ticket that is added to the list of tickets in RSA VA and automatically pushed to the RSA Archer Vulnerability Risk Management solution. In RSA Archer, the ticket becomes a Finding in the remediation workflow. You can see the list of tickets in RSA VA on the Tickets tab.

In the Tickets window, you can select a ticket to review and work with its related content, including its list of issues, their statuses, and a count of issues in each remediation state. You can set and change the ticket assignee and due date, change the ticket status, and remove issues from the ticket or add some issues to a new ticket. You can also view the ticket's corresponding Finding in RSA Archer.

When to Use Tickets to Automate Workflows

You use tickets to automate the workflows for:

- Resolution of vulnerability issues not handled by standard device maintenance processes such as regularly scheduled patch updates.
- Grouping and moving issues requiring formal remediation and exception tracking into the RSA Archer Vulnerability Risk Management solution.

As data flows into RSA VA, you can begin to see patterns in the types of discovered vulnerability issues and how you remediate them. As you become aware of an issue pattern, you can automate discovery and remediation of similar issues with an issue rule that includes a search query to search periodically for the type of issue and creates a ticket to start the remediation process when issues of that type are found.

Issue rules that create tickets are also useful for remediation and exception activities that must be performed and tracked in the RSA Archer VRM solution. For example, your business or industry may require that the remediation of certain types of vulnerabilities be reported and remediated in a very visible way. You can create issue rules that find those vulnerabilities, bundle them into tickets, and push them into the RSA Archer remediation workflow.

An issue rule allows you to set initial attributes for a ticket such as assignee, status, and due date. These attributes are pushed with the ticket to RSA Archer to help direct the next steps in remediation work.

When to Use Tickets to Push Issues into RSA Archer VRM

There are many reasons to create tickets in RSA VA to send a set of issues to RSA Archer VRM. Here are examples of when this is useful:

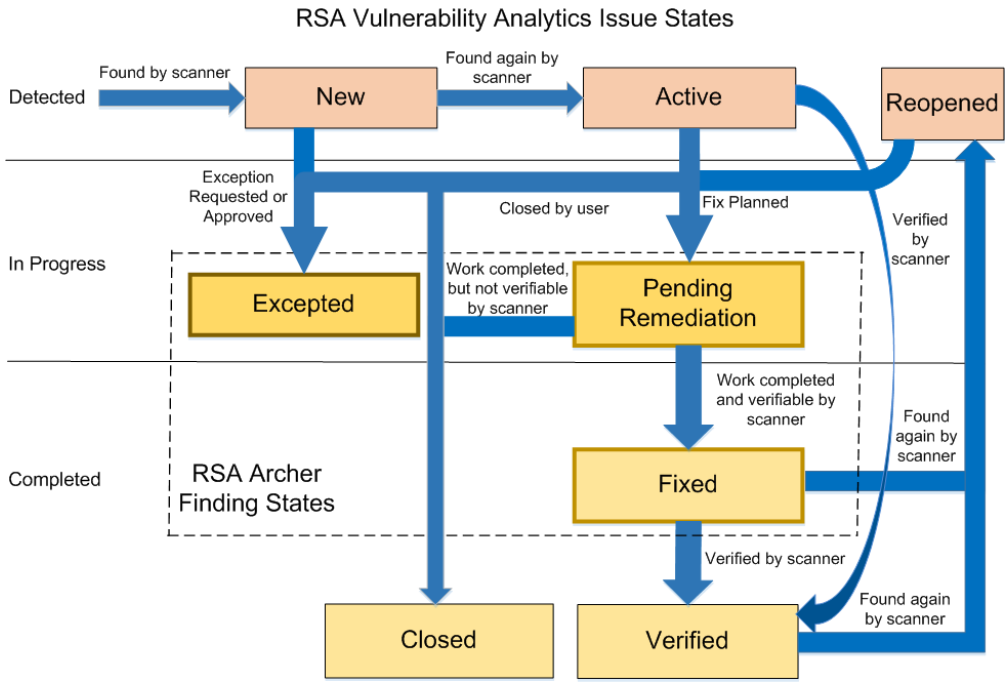
- The issues identified in RSA VA indicate a concern with patching or remediation processes. For example, a recurring vulnerability that should have been addressed by a patch implementation may indicate an issue with the patch infrastructure. To escalate the problem, these issues can be bundled into a ticket and pushed to RSA Archer VRM to highlight and track the root problem.
- Issues that are vulnerabilities found by RSA VA on high risk or critical device assets can be bundled into a ticket and escalated to RSA Archer VRM to ensure close monitoring of the remediation process.
- Issues that are vulnerabilities found by RSA VA that have a changing threat profile can be bundled as a ticket and escalated to RSA Archer VRM to ensure that systems are patched appropriately. For example, a vulnerability that has an open, active exploit may need additional monitoring or tracking to expedite remediation efforts.

The escalation of tickets from RSA VA to RSA Archer VRM should be defined as part of the overall strategy during implementation. The goal of RSA VA is to enable operational processes to identify and patch vulnerabilities. RSA Archer VRM can be used for escalation of operational issues.

Some companies may want to track tickets in RSA VA as Findings in RSA Archer VRM not for escalation reasons, but to provide visibility in the context of other risk processes being managed in RSA Archer. Discussions between security analysts, system owners, and IT management should identify the cases where additional visibility within RSA Archer is warranted and require related tickets to be pushed from RSA VA into RSA Archer VRM.

Issue State Workflow

The following diagram details issue states as they appear in RSA Vulnerability Analytics and as Findings in RSA Archer.



Chapter 5: RSA Archer Vulnerability Risk Management Solution

RSA Archer Vulnerability Risk Management Solution Components

The RSA Archer Vulnerability Risk Management solution is composed of the following components:

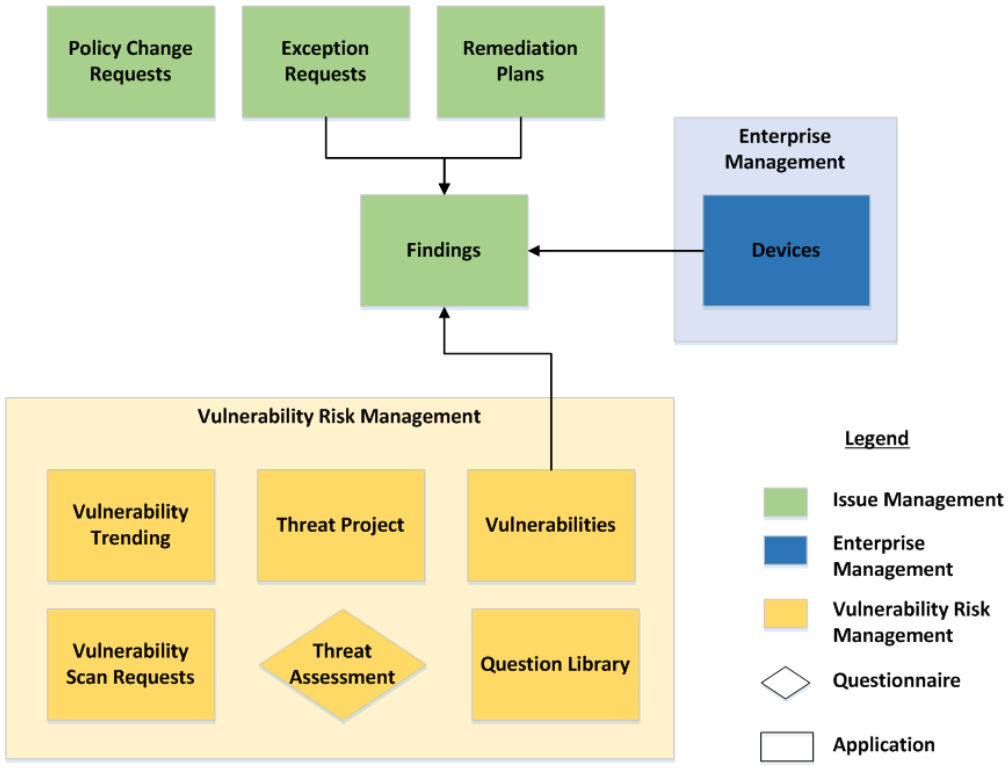
- Access Roles
  - VRM - Archer Admin
  - VRM - Business Manager
  - VRM - Device Owner
  - VRM - IT Executive
  - VRM - IT Security
  - VRM - Read Only
  - VRM - Web Service API
- Applications
  - Devices
  - Exception Requests
  - Findings
  - Policy Change Requests
  - Question Library
  - Remediation Plans
  - Threat Project

- Vulnerabilities
- Vulnerability Scan Requests
- Vulnerability Trending

- Dashboards
  - Remediation Activities
  - Remediation Effectiveness
  - Remediation Trends
  - Scanning Health
- Questionnaire
  - Threat Assessment
- Workspace
  - Vulnerability Risk Management

RSA Archer Vulnerability Risk Management Solution Diagram

The following figure demonstrates the relationships between the Issue Management, Enterprise Management, and Vulnerability Risk Management solutions that make up the RSA Archer VRM solution.



RSA Archer Vulnerability Risk Management Dashboards

Dashboards in RSA Archer VRM give CISOs and executive-level personnel summaries of key performance indicators (KPIs) pushed up from RSA VA. Use the dashboards daily to monitor remediation and scan progress and trends, check for compliance to business processes and time-lines, and look for anomalies that indicate problems requiring additional work, investigation, or process refinement.

You can change the displayed contents of a chart by selecting different data dimension. Dimensions you can select include finding state or assignee, business unit, CVSS score, facility, device group, owner, or type. You can open the detailed data on which the charts are based by clicking a bar or data point.

Dashboards Built into RSA VRM

The initial installation of RSA Archer VRM includes four dashboards containing standard RSA Archer iView presentations of the KPI data uploaded to RSA Archer VRM from RSA VA.

Dashboard	Default iView Contents
Remediation Activities	• Open/Today's RSA Vulnerability Analytics Findings • Findings by State • Exception Requests by State • Remediation Plans by State • Issue State by Dimension Type
Remediation Effectiveness	• Remediation % - Last 30 Days • Average Time to Remediate - Last 30 Days • % Reopened from Fixed - Last 30 Days • % Reopened from Verified - Last 30 Days
Remediation Trends	• Average Finding Age • Average Issue Age - Last 90 Days • Exceptions Trending • Remediation Plans Approved/Completed
Scanning Health	• % Scan Coverage - Last 30 Days • % Authenticated Scan Coverage - Last 30 Days • Average Days to Detect - Last 30 Days

The security analyst who administers RSA Archer VRM can add customized dashboards with targeted content to give frequent users immediate access to only the data they want.

RSA Archer Vulnerability Risk Management Subsolutions and Applications

The RSA Archer Vulnerability Risk Management solution includes the Vulnerability Risk Management and Issue Management subsolutions.

The following applications in the Vulnerability Risk Management subsolution operate in RSA Archer VRM in the same way that they operate in the RSA Archer Threat Management solution:

- Threat Project
- Threat Assessment
- Question Library
- Vulnerability Scan Requests

Vulnerability Trending in RSA Archer VRM

The built-in reports in the Vulnerability Trending application enable you to get a deep understanding of the key performance indicators (KPIs) tracked for vulnerability management. RSA VA pushes the KPIs and supporting data daily to RSA Archer VRM. The CISO and personnel who use these reports in RSA Archer VRM see the same data that the security analyst sees in RSA VA reports.

The metrics are presented in the reports as percentages, averages, and counts of KPIs such as issues remediated and issue statuses, organized by different time periods (daily, weekly, or monthly), and by various data dimensions.

The reports display the metrics as charts and provide tools that let you change the chart forms and appearances. You can drill into the supporting data by clicking a bar or data point. Standard RSA Archer features are available for you to create, modify, save, copy, export, print, and email the reports.

Issue Management in RSA Archer VRM

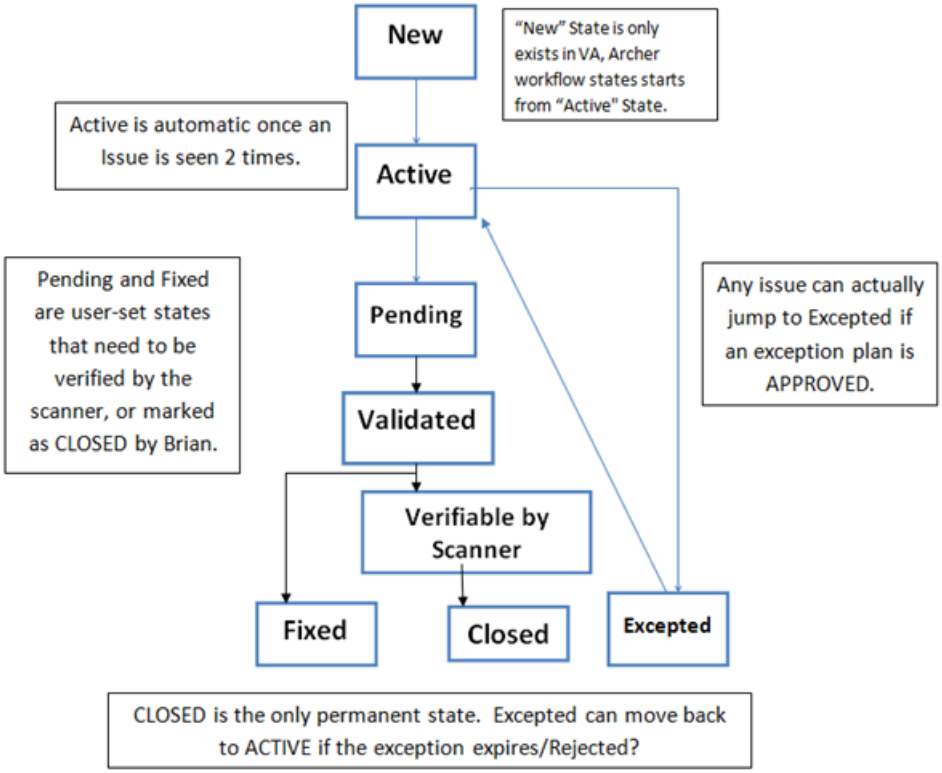
Employees involved in resolving vulnerabilities use the RSA Archer Issue Management subsolution to work through remediation fixes and exception requests. The remediation workflow is driven by progress on Findings.

Each Finding originates as a ticket (a set of issues) in RSA Vulnerability Analytics. After its creation, a ticket can be manually or automatically sent from RSA VA to RSA Archer VRM. In RSA Archer VRM, the ticket becomes a Finding, and is added to the list of Findings in the Issue Management subsolution.

RSA VA also sends the list of issues associated with a ticket to RSA Archer VRM in Microsoft Excel .xls spreadsheet format. The spreadsheet is added to the Finding as an attachment.

RSA Archer VRM Findings Workflow

This diagram highlights how RSA Archer VRM findings are triaged within the RSA VRM solution.



Working with Findings in RSA Archer VRM

You can use standard RSA Archer features to edit a Finding and to export, print, or email the Finding. Depending on your RSA Archer permissions and your role in the remediation workflow, you can edit a Finding to update content such as the assignee and state, and to add comments that document significant progress on the Finding.

The General Information section tells you the Finding's current status, criticality, important tracked dates, and if the current response is to remediate the risk or request an exception.

To see the individuals or teams assigned to work on the Finding, review the Workflow and Description tab.

To see the remediation status and related dates and to access the remediation plan, review the Response tab.

Remediation work for a Finding can involve different steps that must be tracked separately, or done by different people. To see tasks created as work items for the Finding and the progress on, and history of each task, review the Open Tasks/Activities section.

You can add a new task to the Finding, assign it to an individual or group, set a due date for completion, and describe the work you expect the assignee to do to complete the task. As assignees work on and complete their tasks, they can edit their tasks to document the work they have done.

You can see a chronological list of activity related to the Finding in the History Log section. Activity is automatically logged by RSA Archer VRM and maintained as a permanent record of changes to the Finding content.

Remediation Plans and Exception Requests

The issues in a Finding in RSA Archer VRM can be resolved in one of the following ways:

- Issues can be fixed using a remediation process defined by a remediation plan.
- Issues can be declared acceptable risks and not fixed, which triggers an exception request process which requires the reviews and approvals as defined by your business.

The following applications control the remediation and exception request processes in RSA Archer VRM:

- The Remediation Plans application allows you to centrally manage multiple Findings, and track estimated and actual remediation costs and time frames.
- The Exception Requests application allows you to manage the processes of granting and denying exceptions to policies and control standards, and of dealing with expiring exceptions.
- The Policy Change Requests application allows you to document proposed changes to company policies driven by newly discovered or changed issues that must be remediated by business process changes.

These applications operate in RSA Archer VRM in the same way that they do in the RSA Archer Threat Management solution. For information about these applications, see the *RSA Archer Threat Management Overview Guide*.

Issue Status Synchronization Between RSA Archer VRM and RSA VA

Issue statuses are tightly synchronized between RSA Archer VRM and RSA VA so that users of both systems see the same data.

RSA VA sends the initial status of issues and tickets, along with all supporting details, to RSA Archer VRM where each ticket becomes a Finding for remediation work. When the status of a Finding changes in RSA Archer VRM, the status change is communicated to the associated issues in RSA VA.

As vulnerabilities are detected by scanners such as QualysGuard Vulnerability Management or McAfee Vulnerability Manager, RSA VA tracks the status of these Issues over time. RSA VA marks the Issues as Verified once the scanners no longer detect the vulnerability on the device; for example, when Issues are remediated by an automated patching process. When Issues are not remediated in a timely manner, a Ticket can be created to group related Issues together and track the progress of their remediation status. Tickets can be escalated to RSA Archer VRM as a Finding, to track the history of the remediation workflow in finer detail.

You can choose to Accept the Risk that the group of Issues pose for a certain amount of time. For example, you may want to delay patching a set of critical hosts until the next quarter, or until a new software update is rolled out. Choosing to Accept the Risk on the Finding marks the related Issues for the Ticket as Excepted, and sets their Due Date to the Exception Expiration Date. This provides a grace period in which results from the scanners do not reopen the Issue until the time has passed. This also communicates to the Security Analyst that the IT team is aware of the Issue and simply needs more time.

You may alternately choose to Remediate the Risk of those Issues. The features of the RSA Archer Finding track the progress during which a risk remediation plan is defined, tasks are assigned to responsible parties, and the remediation process is approved by a reviewer. Choosing to Remediate the Risk on the Finding marks the related Issues for the Ticket as Pending Remediation, and sets their Due Date to the plan's Fix Date. This provides a grace period in which results from the scanners won't reopen the Issue until the planned Fix Date has passed. This also communicates to the Security Analyst that the IT team is planning to fix the Issue in the future.

Once the approval workflow for the Remediation Plan is complete, the approver can mark whether the Issue is verifiable by a scanner (the typical case), or not. The remediation activity might not be verifiable if it was fixed in a way that the scanner's rules can't detect, or if the scanner is configured with privileged access that an attacker would not have. Marking the remediation activity as complete on the Finding marks the related Issues for the Ticket as Fixed (if it was verifiable) or Closed, and notes the actual Fix Date. This communicates back to the Security Analyst that the IT team has completed their remediation work on the Issue. If scanners continue to detect the vulnerability on that device, the issue is marked as Reopened (for example, if the fix was not complete, or the scanner's detection capabilities have expanded).

Device Synchronization Between RSA Archer VRM and RSA VA

Device information is tightly synchronized between RSA Archer VRM and RSA VA so that users of both systems see the same information.

As part of the initial configuration of the RSA Vulnerability Risk Management product, device information stored in RSA Archer VRM can be pulled into RSA VA and stored in the RSA Analytics Warehouse (MapR). Subsequent scans that find those devices collect technical context (for example, operating system) that is then added to the stored device information. The technical context is then pushed to RSA Archer VRM to synchronize the device information.

If RSA Archer VRM contains additional information about the business context of the device (for example, owner or manager), that business context is communicated to RSA VA and added to the RSA Analytics Warehouse (MapR). A lack of business context information can trigger processes managed by RSA Archer VRM that request business context input from IT personnel. After the business context is added, it is then communicated to RSA VA and stored in the RSA Analytics Warehouse (MapR) to complete the device synchronization.

In RSA Archer VRM, you see the synchronized device information in the Devices application of the RSA Archer Enterprise Management solution.

Chapter 6: RSA Vulnerability Risk Management Use Cases

CVE-2014-0160: Heartbleed

Vulnerability CVE-2014-0160, more commonly known as Heartbleed, is a result of improper input validation of the TLS and DTLS implementations in OpenSSL 1.0.1 Heartbeat Extension packets. This is a buffer over-read, which can allows remote attackers to obtain sensitive information from process memory via crafted packets that would not usually be allowed.

For more information on Heartbleed, visit the National Vulnerability Database website **http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160**.

Use Case: Heartbleed

The RSA Analytics Warehouse (MapR) stores previously gathered scan data in a device inventory. RSA Vulnerability Analytics query engine can be used to search for devices with specific installed software version criteria. This use case shows how you can check for systems that have vulnerable versions of OpenSSL installed if that data has been provided by the scanners.

Procedure

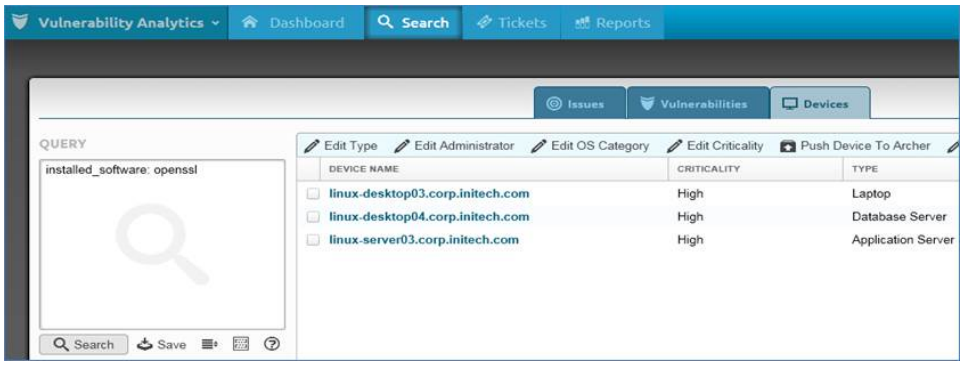
1. Identify the area of concern.

   You want to know whether any systems have been affected by having vulnerable versions of OpenSSL installed.

2. Query for affected systems.

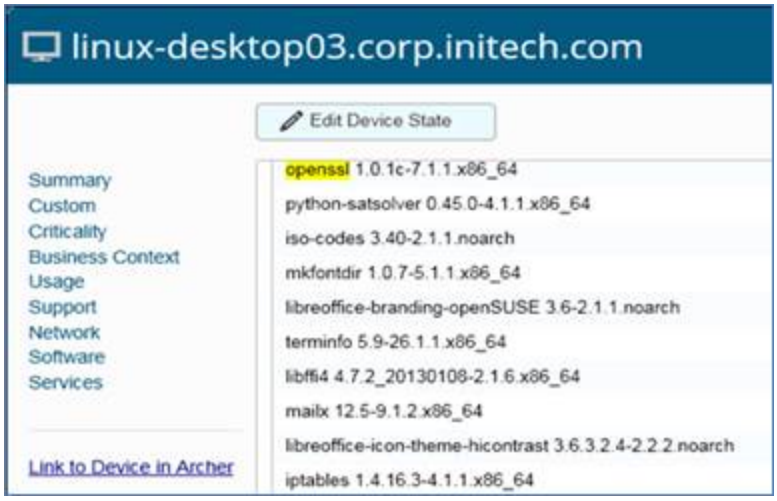
   ```
   installed_software:openssl
   ```

   In the device list, there are 3 devices listed. The two devices witth OpenSSL 1.0.1c are vulnerable. The device with OpenSSL 0.9.8e is not vulnerable.



3. Select one of the vulnerable devices.

   The first device's entry, OpenSSL 1.0.1c-7.1.1 x86_64, indicates that this device is vulnerable and needs to be patched.



4. Refine the query.

   Since OpenSSL 1.0.1g variant is not a vulnerability, the original query can be refined by using Lucene syntax. This new query lists every device with a vulnerable openssl implementation that is in the company's inventory, but excludes the 1.0.1g variant.

   Example Explicit Query:

```
installed_software:"openssl 1.0.1a" OR
installed_software:"openssl 1.0.1b" OR
installed_software:"openssl 1.0.1c" OR
installed_software:"openssl 1.0.1d" OR
installed_software:"openssl 1.0.1e" OR
installed_software:"openssl 1.0.1f" OR
installed_software:"openssl 1.0.1-" NOT
installed_software:"openssl 1.0.1g"
```

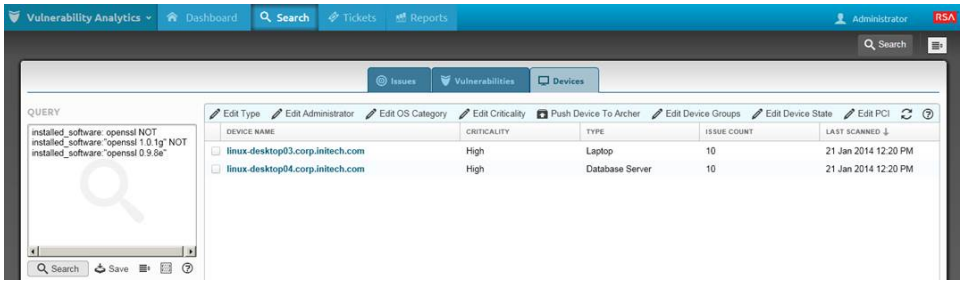
In this example, the 1.0.1g entry is not needed since you are stating exactly what you want listed. You need to know how the record text appears for each of the OpenSSL variants, but once you have an entry in the rule for every vulnerable OpenSSL record, you do not have to continue maintaining the rule as new versions of OpenSSL are released.

If an explicit rule cannot be built, an exclusion rule can be used by adding different versions with a NOT operator.

Example of Exclusion Query:

```
installed_software: openssl NOT
installed_software:"openssl 1.0.1g" NOT
installed_software:"openssl 0.9.8e"
```

5. Review the results of the refined query to find the vulnerabilities.
   With an Exclusion Query, all systems with OpenSSL, except the 1.0.1g variant and 0.9.8e, the variants that are not vulnerable, are listed.



6. Start remediation.
   Once the query is refined, you can create an RSA VA rule based on the query to automatically show alerts in the RSA VA dashboard, and to create notifications. To create a rule after running the query, click  .

   When the Query is saved as a rule, it can be scheduled to run. You can also execute an RSA VA workflow to run all rules at that time to receive an alert and email notification immediately.

   Now you can create and forward a list of systems potentially vulnerable to the Heartbleed vulnerability without waiting on the scan vendor's knowledge base to be updated with the CVE, or for a new vulnerability scan to run.

CVE-2014-6271: Shellshock

Vulnerability CVE-2014-6271, more commonly known as Shellshock, allows attackers to execute malicious bash code through a crafted environment. This allows attackers to obtain sensitive information, make unauthorized modifications, and create a disruption of service. The initial fix for this issue was incorrect and CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the initial failed fix.

For more information on Shellshock, see the National Vulnerability Database website at: **http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271**.

Use Case: Shellshock

RSA VRM can run a query rule to search for all scanned devices that have Bash installed on them. The information on these scanned devices is stored in the RSA Analytics Warehouse (MapR). RSA VRM creates an active catalog of assets that is auto updated and in sync with the network vulnerability that the scanners find.

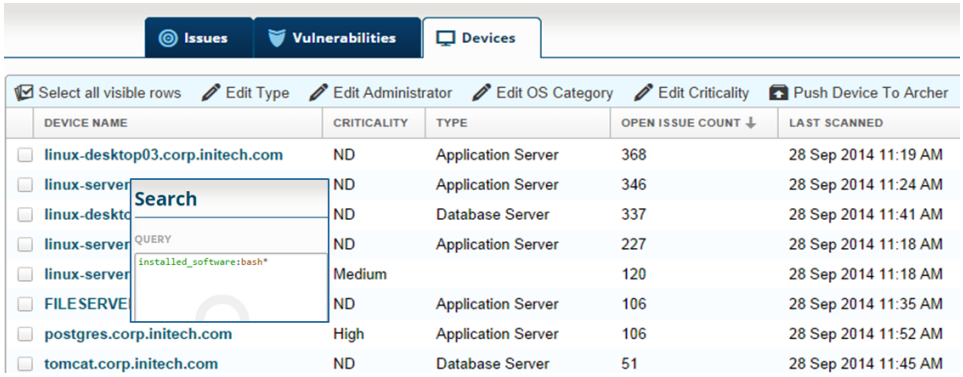
Procedure

1. Identify the area of concern.

   You want to know whether any systems have been affected by having vulnerable versions of Bash installed.

2. Query for affected systems.

   The Security Analyst can run a query to find all devices that have Bash. This provides a starting inventory of vulnerable devices. The Security Analyst can also create alerts in order to monitor the current and newly added devices with Bash on the dashboard.



3. Review the results for all affected systems.

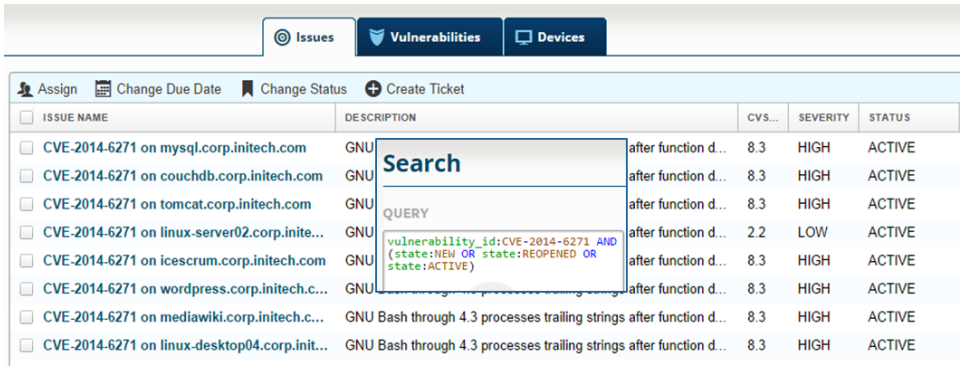
   Once you have identified which devices have Bash installed, check for the devices that have sister shells, such as /bin/sh installed, as sometimes these are copies of Bash. This gives a good initial inventory of devices that may have been impacted by Shellshock.

4. Run a search query.

The Security Analyst runs a search query on devices using CVE ids of Shellshock vulnerabilities. Six vulnerabilities have been identified that are related to Shellshock:

- CVE-2014-6271
- CVE-2014-6277
- CVE-2014-6278.
- CVE-2014-7169
- CVE-2014-7186
- CVE-2014-7187

Four of these vulnerabilities (CVE-2014-6271, 7169, 6277, 6278) are related. CVE-2014-6271 is the key vulnerability amongst these. The others are due to incomplete fixes.



5. Start remediation.

   Prioritize the devices that need to be patched first. RSA recommends that you prioritize these devices based on criticality and business context (who owns the device, risk rating, compliance rating).

   Once prioritization is determined, start a remediation work flow.This provides the necessary foundation to establish the vulnerability management program for Shellshock. As you move through the process, you should consistently be using KPIs to iteratively improve the vulnerability management process.

Appendix A: Differentiating RSA VRM from Other RSA Archer Solutions

How RSA VRM Differs from the RSA Archer Threat Management Solution

RSA VRM is purpose built to manage vulnerability threats. In contrast, the Threat Management solution is designed to manage any threat (geo-political, infrastructural, and vulnerabilities). Also, the two solutions are architected differently in context of location and volume of content that each solution ingests.

Content used by the RSA Archer Threat Management solution resides completely in RSA Archer. The solution uses only standard RSA Archer mechanisms, processes, and storage to manage its threat content. Its scalability is limited to RSA Archer scalability.

RSA Vulnerability Risk Management stores all of its content in the RSA Analytics Warehouse (MapR), which allows it to scale to a very large volume of content. The standalone RSA Vulnerability Analytics component performs the vulnerability risk analysis and prioritization, and the RSA Archer Vulnerability Risk Management solution manages the GRC business side of remediation plans and exception requests.

RSA VRM's ability to consume and analyze large amounts of scan and vulnerability data and to drive remediation of issues prioritized by asset business context makes it the best vulnerability risk management choice for organizations that must protect a large pool of device assets against a constantly increasing flood of vulnerability risks.

The following table compares the features and functionality provided by the RSA Archer Threat Management solution and RSA Vulnerability Risk Management.

Feature of Functionality	RSA Archer Threat Management Solution	RSA Vulnerability Risk Management
Manage threat projects	x	x
Perform threat assessments	x	x
Track threat intelligence	x	x

Feature of Functionality	RSA Archer Threat Management Solution	RSA Vulnerability Risk Management
Build assessment question library	x	x
Track vulnerabilities	Stored in RSA Archer	Stored in the RSA Analytics Warehouse (MapR)
Track malicious code	Stored in RSA Archer	Included in the NIST NVD feed into the RSA Analytics Warehouse (MapR)
Track patch information	Stored in RSA Archer	Included in the NIST NVD feed into the RSA Analytics Warehouse (MapR)
Manage a technology catalog	Stored in RSA Archer	Stored in the RSA Analytics Warehouse (MapR)
Track vulnerability scan requests	x	x
Manage vulnerability scans	x	Stored in the RSA Analytics Warehouse (MapR)
Manage vulnerability scan results	x	Stored in the RSA Analytics Warehouse (MapR) as issues
Manage Findings	x	x - Escalated tickets from RSA VA to RSA Archer VRM
Manage remediation plans	x	x
Manage exception requests	x	x
Manage policy change requests	x	x
Track vulnerability trending and KPIs	---	x
Purpose-built UI for vulnerability analytics	---	x - RSA Vulnerability Analytics

Feature of Functionality	RSA Archer Threat Management Solution	RSA Vulnerability Risk Management
Rules-based grouping and alerting	Uses native RSA Archer notifications	Rules, alerts, and notifications built into RSA VA
Asset management notifications	Uses native RSA Archer notifications	Rules, alerts, and notifications built into RSA VA
Scability	Limited to RSA Archer scalability	Scalable to millions of records daily

RSA VRM Glossary

RSA VRM Glossary

Term	Definition
Apache Avro	A remote procedure call and data serialization framework for Apache Hadoop.
Apache Hadoop	An open source software framework for distributed storage and distributed processing of Big Data on data clusters.
Apache HBase	A column-oriented database management system.
Apache Solr	An open source enterprise search platform.
API	Automated Programming Interface.
CA	Certificate Authority.
CLDB	Container Location Database.
Cluster	A collection of three or more RAW nodes.
CVSS	Common Vulnerability Scoring System used by the NVD to measure a vulnerability's impact.
DLC	RSA Download Central.
FQDN	Fully Qualified Domain Name.
GRUB	Grand Unified Bootloader.
GUID	Globally Unique Identifier.
JSON	JavaScript Object Notation.
KPI	Key Performance Indicator.
LVM	Logical Volume Manager.
MapR	MapReduce. This is the framework used by RSA VRM for processing the large volume of data typically associated with VMS scan outputs.

Term	Definition
NFS	Network File System.
NTP	Network Time Protocol.
NVD	National Vulnerability Database. This database provides updated information on all known vulnerabilities.
OBF	OSM Binary Format.
ODBC	Open Database Connectivity.
OVF	Open Virtualization Format.
RAW	RSA Analytics Warehouse. This may be referenced in other documentation as RSA VRM Data Warehouse (RVDW) or Security Analytics Warehouse (SAW).
RPM	Redhat Package Manager.
RSA Archer EM	RSA Archer Enterprise Management. This is also referred to as one of the core RSA Archer solutions. This is required for RSA VRM to leverage asset data relating to the asset scan results.
RSA Archer VRM	RSA Archer Vulnerability Risk Management. The RSA Archer solution component of RSA VRM. Also referred to as one of the core RSA Archer solutions.
RSA VA	RSA Vulnerability Analytics. RSA VA analyzes the aggregation of data in the RSA Analytics Warehouse to discover and prioritize vulnerability issues for device assets.
RSA VRM	RSA Vulnerability Risk Management. The product as a whole.
SSL	Secure Sockets Layer.
TLS	Transport Layer Security.
UUID	Universally Unique Identifier.
VLAN	Virtual Local Area Network.
VM	Virtual Machine.

Term	Definition
VMS	Vulnerability Management System. This term is used in association with the scanners from Qualys, Nessus, Rapid7, and McAfee.