RSA® Web Threat Detection

Version 6.4

Release Notes

December 2018

This document lists what's new and changed in RSA Web Threat Detection 6.4. The document includes the supported platforms, fixed issues, and workarounds for known issues. Read this document before installation of or upgrade to this version. For specific installation instructions, see the *Installation and Upgrade Guide*.

RSA

What's New in This Release

This release of RSA Web Threat Detection consists of the following changes and enhancements:

CentOS 7 Certification

This release of Web Threat Detection supports CentOS 7, up to and including CentOS version 7.1.

Improved JSON Parsing

This version of Web Threat Detection allows you to configure selectors to choose the parts of the JSON to save to the transaction. Reducing the transaction size improves perfomance by reducing memory and CPU consumption. In previous versions of Web Threat Detection, the entire JSON string of the sniffed traffic was saved to the transaction.

Enhanced IPv6 Support

This release of Web Threat Detection includes full geolocation information for IPv6 traffic, such as city, region, and ISP information, in addition to the IP country that was available for IPv6 in earlier versions.

Page Filtering

This release of Web Threat Detection allows you to filter traffic based on page name, in addition to the existing functionality allowing to filter traffic by page type, reducing the number of processed transactions.

Compatibility and Support

This release supports these operating systems and environment components.

Operating System Support
Web Threat Detection supports the following operating systems and versions:

Operating System	Version
Red Hat Enterprise Linux (RHEL)	6.x up to and including 6.9
CentOS	6.x up to and including 7.1

Browser Support
Web Threat Detection supports these browser versions that support TLS 1.2:

- Internet Explorer 11 or later
- Firefox versions with TLS 1.2 support

File System Support
Web Threat Detection supports these file systems:

- EXT 4
- NFS

Note

Web Threat Detection deployments on CentOS 7 operating systems only support EXT 4 file systems.

Network Support
Web Threat Detection is supported when installed on an IPv4 network.

VMware Support
Web Threat Detection supports the use of RSA Web Threat Detection products with vMware vMotion. Virtual machines running RSA Web Threat Detection processes can be seamlessly moved across physical hosts with vMotion. During such migrations there is no need to restart the processes with the RSA Web Threat Detection applications experiencing minimal data loss.

Java Runtime Environment Support
Web Threat Detection supports these Java Environments:

- Oracle JRE 8
- Oracle JDK 8

Encryption Method Support
Web Threat Detection supports these ciphers:

Cipher	Cipher in TLS/SSL Format
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009D)
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009C)
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
RC4-SHA	SSL_RSA_WITH_RC4_128_SHA (0x0005)
RC4-MD5	SSL_RSA_WITH_RC4_128_MD5 (0x0004)
DES-CBC-SHA	SSL_RSA_WITH_DES_CBC_SHA (0x0009)

RSA Web Threat Detection Documentation

The RSA Web Threat Detection documentation set is comprised of the following documents:

RSA Web Threat Detection Installation and Upgrade Guide

Provides information about system requirements, compatibility and support, and how to install RSA Web Threat Detection.

RSA Web Threat Detection Product Overview Guide

Provides a high-level overview of Web Threat Detection, including system architecture, components, key features and functionality.

RSA Web Threat Detection Release Notes

Provides information about what is new and changed in this release, as well as workarounds for known issues. It also includes the supported platforms and work environments for platform certifications. The latest version of the Release Notes is available on RSA SecurCare® Online at https://knowledge.rsasecurity.com.

RSA Web Threat Detection Security Configuration Guide

Describes the security configuration settings, secure deployment and usage settings, secure maintenance and physical security controls to ensure secure operation of the product.

RSA Web Threat Detection System Administration Guide

Provides information about how to administer Web Threat Detection once it has been installed and configured. This guide is intended for users who make minor configuration changes, monitor system performance and resources, update security certificates, or troubleshoot system behavior.

RSA Web Threat Detection User Guide

Provides information about how to configure RSA Web Threat Detection, perform administrative tasks such as creating and updating users and rules, and monitor the traffic on your website using the Web Threat Detection dashboard.

Installation and Upgrade

The procedures to install or upgrade to RSA Web Threat Detection are described in the RSA Web Threat Detection Installation and Upgrade Guide.

Upgrade Paths

RSA Web Threat Detection version 6.4 supports upgrades from version 5.0.1 and later.

RHEL or CentOS 6

- For Web Threat Detection versions 5.0.1 and later, upgrade to the latest available 6.x version.
- For Web Threat Detection versions 4.6.x and 5.0, first upgrade to version 5.0.1, and then upgrade to the latest available 6.x version.

CentOS 7

- For Web Threat Detection version 6.3 installed on a CentOS 6 server, you must move your Web Threat Detection data from the CentOS 6 server to the CentOS 7 server, then install Web Threat Detection 6.4 and import the data. For more information, see the process for upgrading to Web Threat Detection on CentOS 7 in the *Installation and Upgrade Guide*.
- For Web Threat Detection versions earlier than 6.3, first upgrade to version 6.3 on CentOS 6, and then follow the process of upgrading to version 6.4 on a CentOS 7 server as described in the *Installation and Upgrade Guide*.

Fixed Issues

This section lists issues fixed in this release of RSA Web Threat Detection.

Tracking Number	Description	Resolution
WTD-5535	Application pages contain references to local directory paths on the web server.	This issue is resolved.
WTD-5545	The UI server is vulnerable to a Cross Site Request Forgery (CSRF) CWE 352 attack.	This issue is resolved. RSA Web Threat Detection is no longer vulnerable to these attacks.
WTD-5621	Unscrubbed parameters are used directly in SQL statement executed on the incidents table, allowing SQL injection attacks to the incidents database.	A dynamic query with parameters is used only if the field is allowed to perform updates in the incidents table.
WTD-5626	The FraudAction update script only saves the latest file distributed in the FraudAction Integration feeds, which contains delta updates, and not the entire feed.	The script appends the new files to previously retrieved files and allows the user to configure the amount of time to retain data.

Known Issues

This section describes issues that remain unresolved in this release, with any available workarounds.

Tracking Number	Description	Workaround
WTD-5594	After upgrading to the latest version, when transactions are published from SilverSurfer to the Kafka server, CPU consumption is increased compared to earlier versions for the ActionServer, SilverSurfer, cProfileUpdater and Kafka services.	Customers with traffic that consumes a high percentage of the available CPUs may need to either add additional CPUs, or move some services to additional servers. Perform capacity planning and contact your RSA support representative for assistance.
WTD-5582	Importing a configuration using the Configuration Manager Import function removes all symbols from the `universal.conf` file.	Manually copy the `universal.conf` file instead of using the Import feature.
WTD-5507, WTD-5604	Logs have a maximum limit of 32767 bytes. JSON strings of greater than 32767 bytes do not display in the clickstream.	
WTD-5501	When performing a search for an attribute in the user interface, with a numerical search value that is greater than 20 digits, the search string is truncated to the first 20 digits, and attributes matching the search value will not produce a match.	Add a letter to the attribute value, so that the search treats the value as text string as opposed to a numerical value. The search will return the expected results.
WTD-5391	Silvertap is not able to decrypt ticket resume requests from Microsoft Edge.	
WTD-5353	When an end user begins a transaction near the end of an hour and the transaction ends at the beginning of the next hour, the organizer processes it as part of the second hour's traffic, and it appears in the	Make sure that the system is properly configured so that transactions reach the organizer with no delay.

Tracking Number	Description	Workaround
	clickstream for the second hour. As a result, the transaction is not found when clicked.	
WTD-5326	The RPM is not correctly configured for a complete uninstall.	
WTD-5295	When searching for a transaction using a numeric field and the search value has a leading zero, the search returns meaningless results. For example, a search with "`abi~0123`" will return random results.	Strip leading zeros from the search term.
WTD-5163	If Silver Surfer is started prior to the EDS server, S type data is not included in the transactions. As a result, S type data is not included in scoring and scorelet information for downstream components. This can result in missing data, and the Profile Timeline feature may fail to run.	
WTD-5032	When an attribute is created containing a hyphen (-), the rules engine converts the hyphen to an underscore (_). When a user creates a rule using the attribute, the attribute now contains an underscore instead of a hyphen.	When creating an attribute, do not use a hyphen in the attribute name.
WTD-5010	The change user password event is not logged in audit log.	
WTD-4740	Search fails when a comma is used in the text field.	If the search text contains a comma, search for the text to the point of the comma or after the comma. For example, if the user-agent contains a comma, search for the user agent name up to the point of the comma.
WTD-4661	Threat groups tab is visible in the Administration interface for a multi-tenant environment in tenant mode. The Threat Groups tab should not be visible in this context.	
WTD-4641	In multi-node setup, Scout cannot determine the location of the Configuration Manager. As a result, the 'Go to Configuration Manager' links will not work correctly.	
WTD-4578	When pushing a configuration, sometimes the UI does not display errors.	If an error occurs during a push, review the errors in the syslog which are typically located at /var/log/messages.
WTD-3946	When a report is generating, there is no indication that the report is generating. (It looks as if the report is "hanging".)	
WTD-3923	On running a search with a non-existent attribute (for example, a misspelled attribute or something that does not exist in any of the logs) along with *; search returns all results in the hour, although no entry for the searched attribute exists.	

Tracking Number	Description	Workaround
	This occurs when search is formed using contains asterisk (~*) with a key that does not exist in the logs.	
WTD-3797	Events/keys/attributes with quotes in the name are not handled properly when referred to with $"name" notation in incident details.	Do not include quotes in event, key, or attribute names.
WTD-3381	The login page may show the wrong version number after upgrade.	Clear the browser cache.

Support and Service

RSA Link®	https://community.rsa.com/welcome
Customer Support Information	https://community.rsa.com/community/rsa-customer-support
RSA Ready Community	https://community.rsa.com/community/products/rsa-ready

RSA Link offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Ready Community provides information about third-party hardware and software products that have been certified to work with RSA products. The community includes RSA Ready Implementation Guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

Published December 2018