Release Notes

Published
2022-05-02

JSA 7.5.0 Update Package 1 ISO

Juniper Networks | Engineering Simplicity

Table of Contents

Administrator Notes

About this Installation

These instructions are intended to assist administrators when installing JSA 7.5.0 Update Package 1 by using an ISO file. This ISO can install JSA, JSA Risk Manager, JSA Vulnerability Manager products to version JSA 7.5.0 Update Package 1.

What's New in JSA 7.5.0 Update Package 1

For more information about what's new in JSA 7.5.0 Update Package 1, see What's New Guide.

Installing the JSA 7.5.0 Update Package 1

To install JSA software:

- System Requirements — For information about hardware and software compatibility, see the detailed system requirements in the Juniper Secure Analytics Installation Guide.
- Upgrading to JSA 7.5.0 Update Package 1 — To upgrade to JSA 7.5.0 Update Package 1, see the Upgrading Juniper Secure Analytics to 7.5.0 Guide.
- Installing JSA — For installation instructions, see the Juniper Secure Analytics Installation Guide.

Known Issues and Limitations

The known issues addressed in the JSA 7.5.0 Update Package 1 are listed below:

- When you upgrade to JSA 7.5.0 Update Package 1, the hostcontext service might not start properly, because of signing issues in the JCE Policy files.
- If your network connection is behind a firewall, the App Host is unable to communicate with your Console.

  There is no workaround currently.

- After you install JSA 7.5.0, your applications might go down temporarily while they are being upgraded to the latest base image.
- '9804.install' fails when managed host is removed from deployment before upgrading to JSA 7.5.0.
- If you have WinCollect 7.3.xx installed when you upgrade to JSA 7.5.0, the JSA patch pre-test can fail when the check_yum.sh pre-test does not clean out the old yum cache.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 1 are listed below:

- CVE-2021-3712-OpenSSL as used by JSA is vulnerable to information disclosure.
- CVE-2021-4034-Polkit as used by JSA is vulnerable to privilege escalation.
- CVE-2021-44790, CVE-2021-34798, and CVE-2021-39275-Apache HTTP server as used by JSA is vulnerable to buffer overflow and denial of service.
- Uninstalling a content pack can cause rules to not function as expected.
- Installing a new version of an app can leave the old version still installed and running.
- JSA error when attempting to execute a long AQL query.
- Asset Profiler Configuration ‘Use Advanced’ option changes new input values to a value of zero (0).
- Asset Profiler treats hostnames with different cases (upper and lower) as separate assets.
- Blank Operating System (OS) field displayed for imported assets where the OS is unknown to JSA.
- Attempting to perform a clean vulnerabilities can fail due to a timeout in the backend.
- The clean vulnerabilites function does not work as expected for assets that do not have an IP address configured.
- Updating an asset using the JSA API when the asset has no IP address defined fails with an 'Illegal Argument Exception'.
- Restore fails when deployment configuration is not auto selected when asset data is being restored.
- The Health Metrics log source name from a configuration backup overwrites the new Console's hostname in the log source.
- Hostcontext out of memory can occur when a large certificate revocation list exists.

- Httpd service can fail to start if an issue occurs while installing a new certificate using **install-ssl-cert.sh**.
- Content Management Tool import can change some properties causing saved searches to fail.
- “Optimized” custom event property with different expression types do not properly parse.
- CEP parsing breaks when obfuscation is activated and the CEP has force parsed enabled.
- Regex based data obsfuscation only obfuscates the first data match, not all data matches.
- Event payloads fail to parse correctly when the payload ends in a quotation mark preceded by a space.
- Glusterfs migration manager can fail during rsync of data back to the /store partition.
- Glusterfs migration tool fails when the /store partition encountered is in ext4 format.
- Flows can stop being received by JSA when the ‘FlowGovernor’ experiences a block while trying to connect to ecs-ec process.
- Flow processor process fails to start when the RPM database contains corruption.
- Unable to retrieve maxmind geolite2-city.mmdb updates using a configured proxy in JSA.
- Benign message written to JSA logging on HA secondary: **“[WARN] HA is active but this is not the active box. exiting...”**.
- High Availability Secondary in ‘offline’ state when it is rebooted a few minutes after the Primary during patch process.
- Shutting down the system on a new ISO install before the license agreement causes setup to fail when the system is powered up.
- QNI attempt to connect to license.xforce-security.com after a decapper ran Out Of Memory.
- An API error is generated while using the Log Source Management app when configured to use the ‘norsk (Norge)’ locale in JSA.
- 'An unexpected API error has occurred. please refer to the JSA error logs' when using Log Source Management app.
- Log Source Identifier column displays "N/A" when selected in a log activity page search.
- Intermittent JSA System Notifications 'Time Syncronization has failed - socat failed to initialize' when encryption enabled.
- The offense API updates the offense in the database but the offense manager is not aware of it.

- The JSA Offense model can experience reduced responsiveness after an update is made to a large network hierarchy.
- Flow Processor can sometimes stop processing IPFIX packets sent from QRadar Network Insights.
- Source and destination payloads for ICMP traffic fail to be captured by QRadar Network Insights.
- JSA deploy function can fail to QRadar Network Interface (QNI) appliances after patching.
- Incident Results window can take longer than expected to load.
- Two QNI Tika instances can start on the same port due to a race condition causing repeated messages written to JSA logs.
- Performing a Forensics Recovery can appear to succeed when the task failed silently and never started.
- Higher than expected CPU usage on QRadar Network Insights.
- JSA Risk Manager can display a confirmation message during device import when the devices are not imported.
- JSA Vulnerability Manager report in xls format can fail due to 'NumberFormatException'.
- System Notification stating QVM processor failure to start can be caused by checkQRMLIcenseTrigger in db table.
- Scheduled reports can run on raw data causing them to fail or take longer than expected to complete.
- Routing rule filters drop down list does not reload appropriate options when toggling between online and offline.
- Routing rules with a filter containing a trailing backslash are not editable once saved.
- AQL custom event properties in email templates display as 'N/A' after patching to JSA 7.4.3 or newer.
- Dependent rules are not displayed when reference sets are used in an AQL or ariel filter test in a custom rule.
- Rule owner can fail to be reassigned after a user is deleted.
- Corrupt reference data table can cause the rule wizard to fail to work as expected.
- Rule Response email fails to be sent due to "&" (ampersand) symbol in email address being changed to "&".

- Rules can fail to work as expected due to the accumulator process failing to connect to ecs-ep process.
- When modifying geographic rule conditions under the Spanish locale Belarus is shown as Brasil instead of Bielorrusia.
- Rules can be incorrectly generated in deployments where dual stack is configured and a JSA patch has been applied.
- JSA User Interface rules page can take longer than expected to load.
- JSA Vulnerability Manager (QVM) scan status remains at 'Outside Operational Window' after scan completes.
- When the QVM processor is not running on the console, scan start and stop emails contain incorrect data in subject and body.
- Error message generated in the UI when a security admin attempts to view another user's saved search results.
- Offenses without naming cannot be searched by description.
- Unable to delete an empty Log Source Group due to dependency check fail.
- "Software Install" JSA Event Collector or DataNode can fail to start required services after added to JSA deployment.
- A JSA notification is generated when the autogenerated QRadar_SAML certificate cannot be renewed.
- Notification of dropped flows is not occurring in JSA notifications.
- JSA patching can fail if duplicate IP addresses are present in database table.
- JSA "patch successful with errors" failing on "...9804.install" file.
- JSA patching process can fail on destination site when the Data Sync app is installed.
- JSA patch pre-test can fail due to check_yum.sh issues when WinCollect 7.3.1-16 installed.
- '[Warning] all applicable hosts have migrated from glusterfs to drbd. exiting' when running glusterfs to DRBD migration tool.