IBM Resilient

Incident Response Platform

Release Notes v31

Release Date: October 2018

IBM Resilient Incident Response Platform on Cloud and IBM Resilient Incident Response Platform V31 (on-premises licensed version) orchestrate and automate the people, processes, and technology that are associated with incident response. Purpose-built for either cloud or on-premises environments based on your business needs, these Resilient Incident Response Platform solutions streamline incident response and privacy response management to provide an automatic, fast, and flexible way for organizations to react to events and incidents.

FEATURES AND ENHANCEMENTS

The V31 release of the Resilient Incident Response Platform introduces a number of new features and enhancements. All changes and bug fixes from the previous V30.0 to 30.4 releases are included.

The following lists the new features and enhancements:

- **Localization:** The Resilient user interface and cybersecurity playbooks have been globalized and translated into the various languages. Resilient users can change the language by setting the Web browser to their preferred language. On-premises customers can set the default language for a new organization. The following languages are supported.
  - Japanese
  - Korean
  - Traditional Chinese
  - Simplified Chinese
  - Italian
  - French
  - German
  - Spanish
  - Brazil Portuguese
  - Russian

  Note that some text, such as regulatory and legal-related information, is available only in English.
- **Disaster recovery**: For on-premises customers, disaster recovery deployment options to enable rapid failover in the event of a major infrastructure outage. The Disaster Recovery system is licensed separately.

- **Enhancements to functions and scripting**:
  - Script query builder object that enables users to build queries in scripts.
  - In Resilient scripts (scripts called from rules and workflows, function pre- and post-process scripts, and script conditions in workflows), native Resilient objects are scriptable using Python idioms, including:
    - dictionary operations (keys, items, etc.) for maps
    - list operations (append, pop, sort, etc.) for arrays
    - 'str' and 'repr' for all Resilient objects
  - Script 'log' methods show a representation of objects where previously they might fail with an error.
  - Scripts triggered from a menu-item rule (including scripts in workflows) have access to Activity Fields as a dictionary 'rule.properties'.
  - Scripts in workflows have access to the workflow property-bag, and can iterate over keys that were added by previous steps in the workflow.
- **Dashboard and Reporting changes:**
  - Analytics dashboards include a global dashboard-wide filter to restrict the list of incidents available / displayed in each of the displayed dashboard widgets. Individual widgets can be further filtered as required.
  - Added reporting on average throughput metrics for events and incidents, aiding the measurement of security practitioners' effectiveness.
  - The Dashboard Header widget can be configured with a date range.
  - Incident export to Excel can optionally include attachment information.
- **Privacy**: The following regulators have been updated in the Privacy Module:
  - Peru
  - China
  - South Africa
  - Philippines
  - South Korea
  - Singapore
  - Costa Rica
  - Connecticut
- **Other changes**:
  - Support for handling large numbers of users and group in the user and groups administration pages.
  - Re-organized the Resilient menu bar for improved usability.
  - Support for sending audit data to Splunk Cloud.
  - Added examples and scenarios to the user documentation for usability.

CORRECTED ISSUES

Tracking Code	Issue
RES-4507	REST API: The `GET task: text_content_output_format=` does not apply to task instructions.

Tracking Code	Issue
RES-10140	Previously, calling the data table delete all rows API method on an empty data table returned a 404 HTTP status code (object not found). Now it returns a 200 HTTP status code.
RES-3354	SHA-256 should be the default for signing requests for ADFS.
RES-5036	Return key has unexpected behavior while defining a data table.
RES-5200	Missing scripts are not included in warnings when importing a settings file.
RES-5223	Backup script can fail due to files in use.
RES-5996	resSystemBack -e can fail under certain conditions after upgrading from an earlier version of the Resilient platform.
RES-6085	Bulk reassigning of incidents can be very slow.
RES-7823	Date/Time Values are now stored internally as longs, correcting some edge case behavior when doing arithmetic operations on them in scripts.
RES-8452	Added text to the Create Incident Field dialog to clarify that defaults for multi-select fields apply only when creating an incident and not when editing an incident.
RES-8677	Corrected a concurrency edge case when writing rows to a data table as a result of rule execution.
RES-8722	Firefox browser only: Pasting data from a CSV file into a text box pastes metadata as well as the actual data.
RES-8797	Date picker does not retain a selected time zone.
RES-8835	resSystemBackup -e generates a syntax error.
RES-8945	OVA boot continues even if the Resilient deploy fails.
RES-9133	Tasks added via Automation rules with the condition “incident is created” are removed when the incident is subsequently edited. This should never have been allowed. With this release, it is no longer possible to use the Add Task option in automatic rules for incident type objects if “incident is created” is specified as the condition.
RES-9205	An "incidents_geo_unassigned_inc_id_fkey" foreign key violation error occurs when deleting an incident.

Tracking Code	Issue
RES-9335	Some useful type metadata missing in scripting. Therefore, the following fields have been made available in the type-ahead from scripting: • task.init_date • task.at_id • task.attachments_count • task.cat_name • task.custom • task.notes_count
RES-9343	Interpolated date fields in a pivot table can result in displaying data incorrectly.
RES-9687	Cannot create a SAML federation when the IDP login URL has an invalid top level domain.
RES-9842	Incident fields data are not saved if the Save button is clicked too quickly after editing the textarea.
RES-9873	Cannot use "Tab" to move between Data Table Fields on Task Layout.
RES-9937	attachmb of -1 disallows artifact uploads.
RES-10134	Partial match is used for a "DNS name" typed artifact look-up against the iSight Parter threat feed.
RES-10235	Elastic Search connection is not timing out, possibly leading to leaked threads and an unresponsive server.
RES-11102	Certain dates within the data table date picker field (specifically dates within +- 1 month of 01/01/1970) causes an error.
RES-11217	Customized rules may cause a Quartz job to be scheduled infinitely.

KNOWN ISSUES

Tracking Code	Issue
RES-11325	Using workflow.properties in a workflow function's pre-process script can cause the workflow to fail when the size of the data exceeds 5MB.