IBM Resilient

Incident Response Platform

Release Notes V32.1

Release Date: February 2019

IBM Resilient Incident Response Platform on Cloud and IBM Resilient Incident Response Platform (on-premises licensed version) V32.1 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 V32.1 release of the Resilient Incident Response Platform introduces a number of new features and enhancements. All changes and bug fixes from the previous releases are included.

The following new features and enhancements are provided in Resilient V32.1:

- **Images in rich text**: End users can paste images from screenshots or other sources into rich text fields, including incident and task notes as well as incident fields including custom rich text fields. This feature does not currently include task instructions or rich text fields inside data tables.
- **Menu item rules in the inbox**. Playbook designers can select the email message object type from menu item rules. This allows designers to run a rule against an incoming email so that it creates a user action in an incident. It was previously available only for automatic rules.
- **Last modified date field**. Incidents include a new field called Last Modified which tracks the time of the last change to an incident. It is a read only field that can be used in filters and layouts, and displayed in the incident list. It cannot be used in rules or other conditions.
- **Email notifications**. For new installations, the default is to have users specify which notifications they want to receive. Previously, the default setting was that most email notifications were initially enabled. This does not impact upgrades to existing installations.
- **Phases and tasks page.** The phases and tasks page has been changed to filter out Regulatory / Privacy tasks by default. It is still possible to view these tasks on the page by changing the filter settings.
- **Incident list page changes.** In order to prevent out of memory and / or performance issues, the maximum number of incidents that can be displayed at once is now limited to 500.

- **Export to Excel (Reports).** To facilitate the export of a large number of incidents to Microsoft Excel, the options for the Reports Export to Excel feature have changed. You can now export all selected incidents, or export all incidents that match the current filter. You can use the Export all incidents option to export more incidents than the 500-incident maximum that can be displayed in the incident list.
- **Privacy**:
  - The following regulators were added to the Privacy Module:
    - China (Financial PBOC)
    - Turkey
  - The following regulators were updated in the Privacy Module:
    - Alabama
    - Arizona
    - Guernsey
    - Iowa
    - Liechtenstein
    - Utah
    - Vermont (Data Brokers)
    - Washington
  - The following regulator was removed from the Privacy Module:
    - Experian
  - The layout of the regulator categories, and the regulators listed therein, has been reorganized slightly. This change applies to the Privacy page in the Resilient Wiki, the Regulators page in the New Incident Wizard, and the incident Breach tab.

  PLEASE NOTE: We have removed the calculation and display of ***Estimated Fine Liability***. When breach notification was US state specific and those states gave caps and guidance on fines, this feature had great value. As breach notification has become global with far less guidance as to fines with very high caps, estimating fines has become speculative. Therefore, we will instead focus on other features that we believe are of greater value to our customers.

CORRECTED ISSUES

Tracking Code	Issue
RES-5201	Unable to acquire keyvault lock.
RES-9336	Known causes of the log message "**ERROR c.co3.context.DefaultCo3ContextImpl - Unable to establish context java.lang.IllegalStateException: Max number of active transactions reached:50**" have been addressed.
RES-10277	Localized date-time format is not working in "Custom Range" of "Configure Widget" panel.
RES-10421	"Show All" on the List Incident page can potentially lead to out of memory on server.
RES-11995	Activity fields in menu item rule are not available in event.message.
RES-12381	Slow HTTP POST vulnerability.

Tracking Code	Issue
RES-12519	Incident Type errors during import and export.
RES-12569	VirusTotal cannot be enabled without selecting "Upload files".
RES-12655	Rule runs on a deleted object, and it should not.
RES-12804	User may not see changes to an Incident Note when it is modified by multiple users simultaneously.
RES-12831	Import fails after modifying the role's API name.
RES-12919	Mouse cursor lost for RichText Text Area field in New Incident Wizard.
RES-12932	Resilient makes request for external font files.
RES-13055	Upgrade to v32 docs does not mention new system users needed on the platform.

KNOWN ISSUES

Tracking Code	Issue
RES-13146	If using Safari as the web browser, user cannot paste a screenshot from the clipboard into a rich text field, such as Notes in an incident. Drag and drop of the image works correctly.
RES-13219	Images pasted into incident fields are not shown in the incident report (Chrome only).
RES-13291	Exporting very large numbers of incidents can cause the server to run out of memory, become unresponsive, or both. The exact number of incidents that can cause this problem is dependent on a number of factors including current server load, server CPU capacity and available memory. It is also dependent on the data in the incident.
RES-13370	When a menu item rule condition searches an email body in text/plain format for reserved HTML characters, such as https://, it fails to add the resulting action to the email's Actions menu (on the Mail Inbox page).