IBM Resilient

Incident Response Platform

Release Notes V32.2

Release Date: March 2019

IBM Resilient Incident Response Platform on Cloud and IBM Resilient Incident Response Platform (on-premises licensed version) V32.2 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 V32.2 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 V32.2:

- **Images in Task Instructions**: Administrators can paste images from screenshots and other sources into rich text fields, including Task Instructions. The images are included in exported settings when the Phases and Tasks option is checked.
- **Reference to Wikis from all Rich-Text Fields:** Direct links and references to in-product wiki pages can now be added to any rich text field, including task instructions. This allows for more flexible use of wiki pages, including documentation of response procedures that can be referenced from Tasks.
- **Example Email Processing Script**: The Resilient platform includes a sample script that can parse inbound email messages. Users can edit this script to add an incident owner and optionally add any whitelists. Detailed instructions on using this script are available on the IBM Resilient Customer Success Hub.
- **Security Updates**: The security update for V32.2 addresses various security issues. For on-premises customers, please consult the Resilient Installation Guide for the location of these updates. SaaS customers are updated automatically.

- **Privacy Module**:
  - The following regulators were added to the Privacy Module:
    - **Israel:** *Protection of Privacy Law, 5741-1981 & Protection of Privacy (Information Security) Regulations, 5777-2017*
      - Effective date: May 18, 2018
      - Region: Africa & Middle East
      - Requirements and timing: A 72-hour notice window to Privacy Protection Authority for severe incidents and documentation of all security incidents
    - **Qatar:** *Law No. 13 of 2016 Concerning Protection of Personal Data*
      - Effective date: Jan 29, 2018
      - Region: Africa & Middle East
      - Requirements and timing: There is no reporting timeline in the law but you must report to affected individuals and the Ministry of Transport & Communications.
  - The following regulators were updated in the Privacy Module:
    - **Massachusetts:** *H.B. 4806*
      - Effective date: April 10, 2019
      - Region: U.S. States
      - Requirements and timing: No specific reporting timeline but rolling notification to affected individuals, strict limits on contents of consumer notifications, disclosure of WISP, expanded reporting requirements for the Massachusetts AG & OCABR, and certification that credit monitoring services meet the statutory obligations are all required in the new law.
    - **Arkansas (Insurance):** Updates tasks and Resource Library to align with cross-references to the main Arkansas data breach law.
    - **Wyoming:** Added data types to better align with defined terms and updated notification template for individuals to reflect newly required information.
    - **Wisconsin:** Added data formats to better align with statutory language.
    - **New Hampshire:** Updated language in notification tasks to reflect additional electronic notice options.
    - **South Africa:** Added statutory language to include all defined terms related to breach response.
    - **European Union:** As part of our continuous monitoring effort around GDPR, we make regular updates to incorporate member state implementing laws, links, addresses, and contact information for EU data protection authorities. The following countries had minor updates: *Ireland, France, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Romania, Slovakia, Spain, and United Kingdom.*

PLEASE NOTE: We always appreciate feedback on current legislation and guidance whether it appears in our product or not. Please contact your Customer Relationship Manager if you have any questions about these updates or suggestions for future updates. You can also use the IBM Resilient Community to see how your peers are using IBM Resilient to simplify the complex world of information security.

CORRECTED ISSUES

Tracking Code	Issue
RES-13545	Database deadlock can occur when system is under a heavy load.
RES-13459	Adding large number of Incident and Task comments can significantly lower system performance.
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).
RES-13293	Out of memory error while generating an Incident History Report.
RES-13252	A deleted user is not reactivated correctly using the `resutil newuser` command.
RES-13251	Vague error messages for inbound email rules. The error messages have been improved to make it much clearer that an email is already associated with an incident, rather than showing a generic DAO exception.
RES-13219	Images pasted into incident fields are not shown in the incident report (Chrome only).
RES-13009	The Related Incidents Dialog does not fully display the related artifacts.
RES-12998	Artifact history not included in Incident History details.
RES-12491	No timestamps in upgrade log files.