IBM Resilient

Incident Response Platform

Release Notes v30

Release Date: April 2018

Introducing the next generation of incident response. Intelligent Orchestration dramatically accelerates and sharpens response by seamlessly combining incident case management, orchestration, automation, and intelligence into a single platform. The Resilient next-generation platform is the first to deliver real-time visibility across your SOC tools, quick time to value, and guided response that empowers your team to outsmart, outpace, and outmaneuver cyberattacks.

FEATURES AND ENHANCEMENTS

The V30 release of the Resilient Incident Response Platform introduces a number of new features and enhancements. All changes and bug fixes from the previous V29.0 to 29.4 releases are included.

The following lists the new features and enhancements:

- **Functions:** A *function* is a new object that sends data to a remote component via a message destination. The remote component performs an activity and returns the results to the function. The results can be acted upon by scripts, rules, and workflow decision points to dynamically orchestrate the security incident response activities.

  Playbook designers can create functions in the Functions tab and use them in workflows. As part of the workflow, the designer can add a pre-process script to provide input to the function, and a post-process script to perform an activity in response to the output provided by the function. Designers can also save the output of the function for use later on in the same workflow.

  For integration developers, functions simplify development of integrations by wrapping each activity into an individual workflow component. A function in the Resilient platform sends data to the remote component that performs the activity then returns the results to the workflow. Integration developers can remotely create functions and associated pre- and post-process scripts and workflows then deploy them to the Resilient platform.

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2018. All Rights Reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

- **Workflow enhancements**: Workflows have the following new features that enhance their flexibility:
  - Repeating timers: Allows playbook designers to repeat the occurrence of a non-interrupting timer event.
  - Child Workflows: Allows workflows to be placed within workflows. Playbook designers can better organize their playbooks by creating smaller workflows that perform a smaller, repeatable business process and then use them within more complex workflows.
  - Script conditions: Allows conditions on the output paths of exclusive and inclusive gateways. The condition is a single expression that evaluates to True or False. Playbook designers can add a script that computes a value, which is then consumed by the expression.
- **Wiki:** Users can create and edit wiki pages from within the Resilient platform. This enables organizations to add important information, guidelines, and reference material for the Incident Response team. Wikis can also be used as part of incident response process. All users can access the wiki pages.
- **Workspaces:** Contained areas that can be used to group different categories of incidents for ease of management. Incident managers can assign different incidents to different teams as appropriate. Administrators can assign users to one or more workspaces. Users cannot access incidents in workspaces not assigned to them. Workspaces and workspace roles are now also included in export files when exporting configuration information.
- **Role based access control changes:** The new permissions include the ability to create and manage workspaces, and create and manage wiki pages. As a part of the workspace feature, there is a distinction between Global Roles, which provide user permissions that apply to all workspaces, and Workspace Roles, which grant permissions for the assigned workspace only. Roles are cumulative; therefore, users with Global and Workspace roles have a superset of those permissions. If assigning users to workspaces only, you should remove any assigned global roles. The details are in the *System Administrator Guide*.

  If upgrading to version 30, no changes are made to existing roles. Your administrators need to explicitly grant the new permissions to existing roles.

  For new installations or newly created organizations after an upgrade to V30, the Master Administrator and Administrator global roles have the Manage Workspaces and Manage Wiki Pages permissions assigned by default.
- **Threat source enhancement:** Cisco Threat Grid has been added as a new Threat Source. It is disabled by default.
- **Operating System support**:
  - This release supports the Red Hat Enterprise Linux (RHEL) platform only. For customers on a Debian platform, you need to migrate to V29 RHEL then migrate, as described in the V29 *Installation Guide*.
  - A variation of the Resilient platform that is FIPS 140-2 compliant is available. Please contact Customer Support for details.
- **Documentation**: The *Master Administrator Guide* has been replaced by a *Playbook Designer Guide* and a *System Administrator Guide* to better focus on those user roles.

CORRECTED ISSUES

The following table lists both the new and old codes, as appropriate, for issues.

Tracking Code	Issue
RES-6041 DE3591	Incident fields are not refreshed under the Tasks Tab in Internet Explorer.
RES-6048 DE3600	Failed to log in a local account whose email is the same as Active Directory contact.
RES-7866	Custom field with "Date Picker" type does not reflect the correct time in the EXCEL report.
RES-7895	Conflict error when updating the custom field with wrong type.
RES-8230	"Discard Changes" cannot roll back the filter after navigating away the "List Incidents" page and back.
RES-8250	Locale is not set correctly with browser settings
RES-8578	Resilient platform does not recognize Lets Encrypt Certificates.
RES-8589	Text Area and Text fields cannot wrap text properly for long words.

KNOWN ISSUES

Tracking Code	Issue
RES-7868	Script failure does not terminate a workflow. A workflow that executes a script which fails (for example due to a typo in the script) will not continue, nor will it terminate. The workflow is left in a running state and needs to be terminated manually. Pre- and post-process scripts have the same behavior. To fix this problem, terminate the workflow manually, correct the script and invoke the workflow again.