Aranda Security Compliance

Learn about the latest releases of Aranda Security Compliance (ASEC)

Here you can find information on updates to ASEC functionalities.

Release note 9.5.0

Problem filling in "Minimum version" value in policy

PM-76959-19-202072

In ASEC, when entering a policy with minimum version scanning criteria, as in the case of web browsing with Microsoft Edge; When you set a value for the minimum version, save, exit the policy, and enter again, the value is not preserved.

A setting is implemented to ensure that the minimum version value is saved correctly after exiting and re-entering the policy.

Store Information

CHG-68809-19-301763

- Date of recent vulnerabilities

Functionality is implemented to capture and log the most recent vulnerability creation and update dates. This allows for improved accuracy and traceability of information, ensuring that data accurately reflects the current state of detected vulnerabilities.

Thanks to this improvement, the information necessary for the generation of the Recently Discovered Vulnerability Report, which provides a detailed list of vulnerabilities identified within a parameterizable period. This report facilitates risk analysis, strategic safety decision-making, and timely corrective action planning.

In addition, with the updated record of creation and modification dates, the monitoring of vulnerabilities over time is optimized, allowing trends to be evaluated, the effectiveness of mitigation actions to be measured and to ensure more efficient management of security in systems.

- Compliance history for a group

Functionality is implemented to record and manage the compliance history of the groups associated with the policies. This allows compliance levels to be stored and tracked over time, providing detailed information on their evolution.

Thanks to this implementation, it will be possible to generate the Compliance Report, which will provide a comprehensive view of the status of each group in relation to the established policies, facilitating analysis, auditing and strategic decision-making.

- User who performed the remediation

The registration of the user performing the remediation is implemented in the device detail. This functionality allows for improved traceability of the actions taken, providing greater visibility into who executed each remediation and at what time.

Thanks to this record, it is easier to track the interventions carried out on the devices, which contributes to better audit management and allows informed decisions to be made based on the history of actions. This helps to strengthen control and security in remediation processes.

MetaData Auto-Update

- A functionality is implemented that allows the automatic update of the MetaData by Operating system. This process takes care of loading, processing, and updating information in the database, ensuring that the data accurately reflects the latest state of each operating system.

With this improvement, the management of the MetaData, ensuring that any changes or new information related to operating systems are processed efficiently and without manual intervention. This not only improves the integrity and consistency of the data, but also makes it easier to make it available for analysis, reporting, and auditing.

In addition, by automating this process, the risk of human error is reduced, operational efficiency is improved and maintenance and information updating tasks are streamlined, providing a more reliable and up-to-date database for strategic decision-making.

New Remediation Activity Functionality

- The Remediation Activity, as part of the Devices detail, presents the history of remediation activities generated by discovered security issues.

For more details, please refer to the following documentation:

- Remediation ↪ Activity

New functionality: export list vulnerabilities and devices

CHG-66794-19-301717

- The action to Export the list of vulnerabilities and detected devices enables security analysis and audits, and facilitates the organization and monitoring of the technological infrastructure. The export of vulnerability and device lists can be generated in compatible formats such as CSV or Excel, improving efficiency in the management and reporting of critical data.

For more details, please refer to the following documentation:

- Export List of Vulnerabilities ↪
- Export Device List ↪

Improved Filter Policies

- The advanced policy filter is implemented with options to perform queries by Operating System and by associating devices to policies.

For more details, please refer to the following documentation:

- Policy Filter ↪

Additional Notes or Instructions

- Automatic agent update requires the services of the common.

- ASEC is released with common version 9.9.1.6
- ASEC released with database version 9.5.48

⚠ Important: In joint installations between Aranda products, you must have the same compatibility as the Common version.

Release note 9.4.2

New Device Delete Functionality

CHG-66615-19-301711

- The new device removal functionality allows users to manage and clean their inventory faster and more efficiently. It is now possible to select and remove multiple devices simultaneously, simplifying the process and saving time. In addition, this feature includes the option to uninstall the agent from the computer in the same step, ensuring a complete removal of the system. This is especially useful for maintaining an up-to-date environment with no outdated or unauthorized agents on devices.

Improves vulnerability detail

CHG-65315-19-301690

- Each Vulnerability provides a more complete and accessible detail on each detected threat. It includes clear fields for the description of the vulnerability and the affected software, making it easier to understand the scope of each risk. In addition, it provides references to advisories, solutions, and recommended tools to mitigate the vulnerability. An additional filter allows you to display the specific devices that contain this vulnerability, along with the date of publication and last update. These updated details help prioritize the response to each vulnerability based on current criticality and relevance.

Additional Notes or Instructions

- Automatic agent update requires the services of the common.

- ASEC is released with common version 9.9.1.6
- ASEC is released with database version 9.5.47

⚠ Important: In joint installations between Aranda products, you must have the same compatibility as the Common version.

Failure to associate devices with a fulfillment group

PM-73597-19-201986

An error was identified in the ASEC console, in the compliance groups module, where it was not possible to associate devices to the corresponding groups. As a result, a correct assignment of devices was not carried out, affecting the management and compliance of policies in the system.

Adjustment is implemented that allows devices to be successfully added to compliance groups, ensuring more efficient management aligned with platform requirements.

Release note 9.4.1

Improved Device Listing

- In the list, the icons have been redesigned to identify devices that have not been scanned and those that do not present vulnerabilities. These categories are added to the filters to improve ranking.

Agent Enhancement

- An agent version is generated to optimize performance on devices.

Additional Notes or Instructions

- Automatic agent update requires the services of the common.

- ASEC is released with common version 9.9.0.11
- ASEC released with database version 9.5.46

⚠ Important: In joint installations between Aranda products, you must have the same compatibility as the Common version.

Release note 9.4.0

New Vulnerabilities Functionality

CHG-49175-19-301403

- New vulnerability detection functionality allows you to proactively identify and manage potential security threats. With this system, the agent reports the scanning of the device every 24 hours, detecting vulnerabilities known by their respective CVE. This makes it easier for IT administrators to take preventative measures to protect data and maintain the integrity of systems. This tool is essential to strengthen cybersecurity and reduce the risk of attacks.

Module Improvement Summary

CHG-52915-19-301494

- The Summary module has been improved so that clicking on any of the three panes: “Policy Compliance by Device”, “Installed Agents”, and “Policy Status” will display more detailed information. This to facilitate access and management of this information.

Additional Notes or Instructions

- Automatic agent update requires the services of the common.
- ASEC is released with common version 9.9.0.11
- ASEC is released with database version 9.5.45

⚠ Important: In joint installations between Aranda products, you must have the same compatibility as the Common version.

Release note 9.3.0

Licensing module improvement

CHG-53037-19-301517

- The licensing module is adjusted to show only the concurrent users option in the “Users” column, because it does not apply to named users.

Improved Policy Management Module

CHG-53038-19-301518

- The “Policy Groups” module in the “Settings” menu is renamed to “Compliance Groups” to give more context to the functionalities of the section, since here the devices are grouped to associate them with the policies.

Configure: Policy validation for macOS and Linux

CHG-49172-19-301402

For this release, the following adjustments were made:

- This release configures the console to perform policy validations on macOS and Linux operating systems.
- Versions of the Agent are created for macOS and Linux.

Additional Notes or Instructions

- Automatic agent update requires the services of the common.
- ASEC is released with common version 9.8.1.2
- ASEC released with database version 9.5.43

⚠ Important: In joint installations between Aranda products, you must have the same compatibility as the Common version.