Micro Focus Security
ArcSight Compliance Insight Package

ArcSight ESM 6.8c, 6.9.1c, 6.11.0

Release Notes

Document Release Date: August 31, 2019
Software Release Date: August 31, 2019

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

CIP for PCI 4.1

The Compliance Insight Package for the Payment Card Industry (CIP for PCI) provides a system of reports and real-time checks specifically designed to monitor systems that contain cardholder data, manage vulnerability and access control, monitor networks, and maintain security policies to help demonstrate to stakeholders and auditors that the controls over your company's credit card data systems expose little or no risk.

CIP for PCI 4.1 coupled with ESM can assist you in complying with the PCI requirements specified in Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 and includes support for logs generated by payment applications subject to the Payment Application Data Security Standard (PA DSS) 3.2.

What's New in CIP for PCI 4.1

CIP for PCI 4.1 includes the following changes:

- Additional support for the following PCI 3.2.1 requirements :
  4.1.1, 6.4.5, 8.3.1, 10.8, 11.3.4.1, and 12.4
- Support for the PCI DSS 3.2.1 and PA DSS 3.2

Requirements

CIP for PCI 4.1 is supported on the following ESM releases:

- ESM 6.11
- ESM 6.9.1c
- ESM 6.8c

Release Contents

The files included in this release are:

File name	Description
ESM_PCI_Solution_ ReleaseNotes_4.1.pdf	This document. Product description and open issue.
ESM_PCI_SolutionGuide_ 4.1.pdf	*ArcSight ESM Compliance Insight Package for Payment Card Industry 4.1 Solution Guide* Product architecture, installation, configuration, and operation instructions with a description of product contents.
ArcSight-ComplianceInsightPackage-PCI.4.1.0028.0.arb	Installable package bundle for all operating systems. Contains all the resources of the Compliance Insight Package for PCI. **Note:** If you use Internet Explorer to download the ARB file, it may convert the ARB file to a ZIP file. If this occurs, rename the ZIP file back to an ARB file before importing into ArcSight ESM.

Installing CIP for PCI 4.1

CIP for PCI 4.1 is for fresh installation and also for upgrade from PCI 4.0.

Complete installation, upgrade, and configuration instructions for the Compliance Insight Package for CIP are located in the document called ***ArcSight ESM Solution Guide Compliance Insight Package CIP 4.1*** (ESM_PCI_SolutionGuide_4.1.pdf).

Caution: You can install CIP for PCI alongside other solutions on the same ArcSight ESM Manager.

However, due to the extensive redesign of CIP for PCI 4.x, there is no migration path from earlier versions of CIP for PCI, such as CIP for PCI 3.0 or CIP for PCI 3.01. If you are running an earlier version of PCI and you need to keep your current data, do not uninstall the earlier version; instead, install CIP for PCI 4.x on a different system.

Performance Impact

ArcSight ESM Solution Packages contain data monitors and rules that can place an additional load on the ArcSight ESM Manager, which may impact the ArcSight ESM Manager performance. If your ESM system is operating at an average event per second (EPS) rate that has maximized the CPU utilization, you might experience a reduced average EPS rate after installing the CIP package. If this performance impact occurs, consider disabling unneeded data monitors and rules to reduce the load on the Manager.

Open Issues in this Release

This release contains the following open issues.

Number	Description and Workaround
SOL-3913	In ArcSight ESM 6.8c and later, the following rules are CPU intensive and might affect system performance. /All Rules/Real-time Rules/CIP/Compliance Scenarios/Network Security/ Network IDS Detected /All Rules/Real-time Rules/CIP/Compliance Scenarios/Monitoring/Non-empty Origination of Event /All Rules/Real-time Rules/CIP/Compliance Scenarios/Monitoring/Events from External-Facing Technologies /All Rules/Real-time Rules/CIP/Compliance Scenarios/System Hardening/Multiple Functions Implemented on a Server /All Rules/Real-time Rules/CIP/Compliance Scenarios/Network Security/Private IP Protected From Disclosure Workaround: Change the rule's aggregation Time Frame setting from 2 to 5 minutes. Refer to the ArcSight Console User's Guide, topic on "Aggregation Time Criteria," for details.
SOL-3836	On high EPS systems, certain query viewers might not return data and some reports take a long time to run. Workaround: Edit the query viewer and the report to change the interval to one hour by setting the Start Time and End Time parameters.
SOL-3594	For certain rules, the AssetName, AssetID, and AssetZone local variables are not resolved; therefore, the `All Active Lists/ArcSight Solutions/CIP/General/Compliance Score` active list displays $AssetName, $AssetID, and $AssetZone instead of the actual asset name, ID, and zone.
SOL-5151	On high EPS rates, the Data Monitor: /All Data Monitors/ArcSight Solutions/CIP/Regulations/PCI DSS/PCI DSS Compliance Score: Top Level could affect ESM Manager performance because this Data Monitor works with all the events. Workaround : Limit the data monitor filter to your specific environment like CDE Assets , reporting devices.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (Compliance Insight Package for PCI 4.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to mailto:arcsight_doc@microfocus.com.

We appreciate your feedback!