GRSEE Compliance ASAP.

Akamai

PCI DSS v.4 Whitepaper

November 30, 2023

GRSEE Compliance ASAP. Akamai

Versions

Author	Role	Date	Description
Talia Goldich	QSA & Information Security Consultant	30-Oct-2023	Initial Draft
Amir Berkowitz	QSA & Information Security Consultant	30-Oct-2023	Tech QA
Sharon Gendelman	Technical Writer	31-Oct-2023	QA
Talia Goldich	QSA & Information Security Consultant	16-Nov-2023	Second Draft
Thomas Craft	Technical Writer	30-Nov-2023	QA

Notice! This report may contain confidential corporate and/or sensitive PII data regarding business flows and working procedures. The customer is advised to keep the document within the organization in a safe location.

GRSEE Compliance ASAP. Akamai

Table of Contents

1 Executive Summary

1.1 Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a global set of security standards defined by the Payment Card Data Security Council to protect payment card data against evolving cybersecurity threats. Any organization that stores, processes, or transmits payment cards online, from small start-ups to large global enterprises, must adhere to each requirement outlined in PCI DSS to remain compliant and avoid penalties. Released in March of 2022, version 4.0 of PCI DSS introduces several new security requirements, including the need for organizations to actively manage and protect against JavaScript threats on the client side. IT managers, security teams, and internal auditors can benefit from the use of Akamai Client-Side Protection & Compliance to accelerate compliance with version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS) by providing the auditor with comprehensive real-time and historical visibility of JavaScript execution behaviors, assisting security teams in detecting and mitigating client-side data breaches, as well as addressing two critical JavaScript security requirements with one solution.

Meeting all the requirements outlined in PCI-DSS v4.0 and achieving certification puts a significant burden on organizations.

1.2 Background

Akamai provides a platform for cloud computing, security, and content delivery. In 2023, Akamai contacted GRSee Consulting Ltd. requesting an assessment and documentation of the security status of a core web application security product, Akamai Client-Side Protection & Compliance, as it compares to PCI -DSS v4.0. The GRSee Consulting QSA has examined Akamai Client-Side Protection & Compliance (CPC), mapping to PCI DSS v4.0 for assessment.

2 Introduction

2.1 Designated Recipients

This whitepaper provides information to IT managers and PCI internal auditors to better understand network security needs and best practices to mitigate payment data threats and the related requirements for PCI DSS version 4.0 audits. Akamai helps to provide visibility for PCI internal auditors, IT managers, and their network operation teams to design, plan, and integrate the changes required for PCI DSS compliance into business-as-usual activities.

2.2 Scope and Responsibility

This document is for IT managers and PCI internal auditors of Akamai Client-Side Protection & Compliance (CPC). The purpose of this document is to provide guidance on which specific capabilities of the solution address certain tasks and requirements of PCI DSS v4.0. Akamai Client-Side Protection & Compliance helps organizations meet the criteria for an external audit and reduce the risk of JavaScript threats, such as web skimming or Magecart-style attacks, which aim to steal end-user data from the client side. The testing was performed by a QSA (Qualified Security Assessor) in a demo environment of Client-Side Protection & Compliance. It is the customer's responsibility to test the suitability of their environment for implementation.

2.3 Terminology

Cardholder Data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.

Payment Page: A web-based user interface containing one or more form elements intended to capture account data from a consumer or submit captured account data. The payment page can be rendered as any one of the following:

- a single document or instance;
- a document or component displayed in an inline frame within a non-payment page;
- multiple documents or components, each containing one or more form elements contained in multiple inline frames within a non-payment page.

Payment Page Scripts: Any programming language commands or instructions on a payment page that are processed and/or interpreted by a consumer's browser, including commands or instructions that interact with a page's document object model. Examples of programming languages are JavaScript and VB script; neither markup languages (for example, HTML) nor style rules (for example, CSS) are programming languages.

PCI QSA: A PCI Qualified Security Assessor is the only entity that can assess and certify PCI DSS compliance; the PCI Council maintains a current list of approved assessors.

GRSee Consulting is a QSAC (Qualified Security Assessors Company). A QSA has performed the whitepaper for Akamai Client-Side Protection & Compliance. For further information regarding our certification, please contact us at:

GRSee Consulting Ltd.

Eli Horovitz 19 St.

Rehovot, Israel 7608802

Email: Info@grsee.com

Phone: +972.8.866.1155

Fax: +972.8.9464051

3 Assessment Results

For each paragraph of the requirement, the following table details whether Akamai meets, supports meeting, or supports the efforts of validating compliance.

1. **Meets** - Using Akamai Client-Side Protection & Compliance (CPC) allows for meeting a specific requirement.
2. **Supports** - Using Akamai Client-Side Protection & Compliance (CPC) supports efforts in meeting a specific requirement.
3. **Validates** - Using Akamai Client-Side Protection & Compliance (CPC) supports validating compliance with a specific requirement.

Section	Requirement	Meets	Supports	Validates
Maintain a vulnerability management program	Develop and Maintain Secure Systems and Software	6.4.3	6.4.3	
Regularly monitor and test networks	Test Security of Systems and Networks Regularly	11.6.1		

3.1 Akamai Client-Side Protection & Compliance Description

Akamai Client-Side Protection & Compliance's PCI Client-Side Protection dashboard outlines four key categories as they relate to JavaScript security requirements 6.4.3 and 11.6.1:

- Client-Side Script Inventory - Provides an inventory of all scripts executing its collected data on defined payment pages, including URLs and script behaviors, and allows users to provide written justifications for every script. This section includes three (3) categories of script inventory status:
  - Known vendor scripts - Categorization of scripts across third-party vendors known to Akamai. Users can leverage pre-built justifications provided by Akamai to auto-justify a particular script or override it manually.
  - Unknown vendor scripts - Categorization of scripts across third-party vendors unknown to Akamai. Users must provide manual script justification for individual scripts. However, the solution allows users to create custom rules that enable automatic script justification across multiple scripts that cover the same pattern simultaneously.
  - First-party scripts - Categorization of scripts that come from first-party code. The solution allows users to provide justification across individual scripts or create custom rules to automate and apply justifications for multiple scripts simultaneously.

- Script Authorization - Provides insight into all scripts authorized or unauthorized to run on defined payment pages. It considers any script that lacks written justification as a part of client-side script inventory to be unauthorized and presents this information as a part of the dashboard. Users receive routine alerts for unauthorized scripts via email notification.
- Payment Pages Protection - Provides tracking of all script execution behavior on payment pages to identify anomalies. Users can immediately respond to unauthorized changes or modifications to HTTP headers on payment pages. It detects when the solution no longer protects specific payment pages. Dedicated alerts provide users with notification regarding any tampering of any defined payment pages and unauthorized modifications for immediate mitigation.
- Script Integrity - Provides tracking and analysis of all JavaScript execution behavior on payment pages. Dedicated alerts notify users of any script integrity violation, detailing anomalous behavior demonstrated by a particular script for immediate mitigation.

3.2 Maintain a Vulnerability Management Program

PCI-DSS Requirement 6.4.3 - Payment page scripts loaded and executed in the consumer's browser are managed

Clause 6.4.3 of the standard requires that all payment page scripts loaded and executed in the consumer's browser be managed as follows:

- A method is implemented to confirm that each script is authorized.
- A method is implemented to ensure the integrity of each script.
- An inventory of all scripts is maintained with written justification for why each is necessary.

During the assessment, the QSA examined Akamai Client-Side Protection & Compliance and validated that:

- Akamai Client-Side Protection & Compliance supports managing and authorizing an inventory of payment page scripts. The QSA observed that the solution identifies all scripts that execute on the defined payment pages and presents detailed information in the Akamai PCI Client-Side Protection dashboard. The solution's Client-Side Inventory provides an inventory of all JavaScript executing on payment pages and allows users to log business justifications for each identified script manually or in an automated manner. The Client-Side Inventory also categorizes observed scripts by known, unknown, and third-party scripts. For scripts sourced from third-party vendors known to Akamai, users can leverage predefined justifications or override with manual justifications to justify scripts. Scripts sourced from vendors unknown to Akamai and third-party(s) can be justified manually by individual scripts, or users can leverage custom rules to apply justifications for auto-generated and multiple scripts simultaneously.
- Akamai Client-Side Protection & Compliance meets ensuring the integrity of each script executed on defined payment pages. The QSA observed that the solution tracks and analyzes the execution behavior of payment scripts in real time. It provides dedicated alerts to notify users of suspicious behavior with insights for immediate response and mitigation.

3.3 Regularly Monitor and Test Networks

PCI-DSS Requirement 11.6.1 – Change- and tamper-detection mechanism

Section 11.6.1 of the standard requires that a change- and tamper-detection mechanism is deployed as follows:

- The mechanism is configured to alert personnel of unauthorized modifications (including indicators of compromise, changes, additions, and deletions) of the HTTP headers and the contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP header and payment page.
- The mechanism functions are performed at least once every seven days OR periodically.

During the assessment, the QSA examined Akamai Client-Side Protection & Compliance and validated that it **meets** the change-detection mechanism by monitoring the execution behavior of scripts on payment pages and alerts in case of abnormal behavior. The monitoring includes modifications of the HTTP headers and the contents of payment pages.

4 About Us

4.1 About GRSee

GRSee Consulting was established by a team of security experts with interdisciplinary knowledge and vast experience in the field of information security. GRSee Consulting provides numerous services in the fields of information security, application security, penetration testing services, cyber services, APTs, threat-modeling, secure architectures & design, and multi-regulation enterprise environments.

GRSee Consulting provides consulting, testing, and certification services in the fields of cybersecurity, information security, and compliance.

The company provides a range of security services to myriad organizations in multiple fields, including Enterprises, Fintech, Hitech, Payment Gateways, Online Gaming, Forex, Financial, and Insurance. Among our core services are the following:

- Audit & regulations – PCI DSS, ISO 27001, ISO 27799, GDPR, HIPAA, WLA.
- Risk assessments – custom risk assessments for sectorial regulators (Banking oversight & Insurance oversight).
- Information security services such as – black/ grey/ white box penetration testing, risk surveys based on various security frameworks, and gap analysis.
- Ongoing consulting services.
- Training – global training and awareness projects & in-depth training for developers/ QA team and other focused groups.
- Professional services – implementing policies on various security products across organizations (DLP, SIEM, endpoint security, deception, etc.).
- Outsource & placement – GRSee Consulting has an independent unit that deals with recruiting employees whether under an outsourcing agreement or a placement contract for our customers.

4.2 QSA Acknowledgment

The QSA Company assures that the information stated above is applicable to version 4.0 of the PCI DSS Standard and the date of the assessment.

Assessment Date: October 16, 2023

Lead QSA Name: Ms. Talia Goldich (Certificate Number 205-996)

Signature: 

Digitally signed by *.grsee.com
DN: CN=*.grsee.com
Reason: I am approving this document
Location: USA
Date: 2023.12.11 20:16:13-05'00'