AKAMAI KONA SITE DEFENDER (KSD) SERVICE IMPACT LEVEL 2 (IL2) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

12 September 2017

Developed by Akamai Technologies, Inc. and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Akamai Kona Site Defender (KSD) Service Impact Level 2 (IL2) Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the Akamai KSD configuration and administrative web portal access. The Akamai KSD is a cloud service providing web application firewall (WAF) protections inline between web servers and users.

This Akamai KSD Service IL2 STIG provides technical guidance for configuring the management portal and the WAF itself. The management portal guidance is based on the Network Device Management (NDM) Security Requirements Guide (SRG), which covers authentication, authorization, audit, and user access. The WAF, to include the optional Client Reputation module, is based on the Application Layer Gateway (ALG) SRG, which includes reverse proxy, protocol/port filtering, and protocol header inspection.

The scope of the Akamai KSD Service IL2 STIG limits implementation to Impact Level 2 as defined in the Cloud Computing SRG. For implementations of higher Impact Levels, further risk evaluation will need to be performed using the ALG SRG requirements for those intermediary services implemented, such as remote access control and user authentication/authorization. Further, higher Impact Levels must meet the requirements set forth in the Internet NIPRNet DoD DMZ STIG.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that “all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures” and tasks that Defense Information Systems Agency (DISA) “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not

applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

The Akamai KSD is a cloud computing service providing WAF functionality and Client Reputation. Configuration of the WAF cloud service is performed through the Luna Portal or Akamai Professional Services. Those performing assessment will access the configuration settings through one or both of these methods.

2.1 Akamai Professional Services

Akamai Professional Services provides support services for KSD to configure details of the Kona Rule Set (KRS) and other configuration settings. Akamai Professional Services is integral to setting up an instance of the KSD, including the initial KRS settings. Additionally, Akamai Professional Services is the only means to set user password requirements for Luna Portal users. Current configuration settings can be retrieved and modified by Akamai Professional Services.

2.2 Accessing Luna Portal

The Akamai Luna Portal is the web access portal for administration of the Akamai products. Most configuration settings can be performed by accessing the Luna Portal via the web.

2.2.1 Single Sign-On Using SAML

The Luna Portal supports SAML 2.0 Integration for fully federated control of users, single sign-on, and multifactor authentication. This solution, for customers using their own identity provider, validates the user's identity prior to allowing access to Luna Portal. Implementing SAML is required by the Akamai NDM STIG.

2.2.2 Account of Last Resort

An Account of Last Resort (ALR) is often used with network devices as a means of providing access in the event critical configuration changes are immediately mandated and network access is not available for authentication. However, when a Service Level Agreement (SLA) provides for 24/7 access to Akamai Professional Services for configuration, an ALR is no longer required within DoD.

2.3 Intermediary Service

An intermediary service is a Web service that is invoked in a chain, such as an XML gateway that receives requests from requesters, performs security checks against the requests, and then forwards the requests to an internal Web service provider. From the perspective of the requester, there is only a single provider, but in reality there are two. any number of intermediary services may be involved in a single Web service transaction. Examples of intermediary services include remote access, user access control, and user authentication. These intermediary services are beyond the scope of the Akamai KSD Service IL2 STIG.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Overview

The Akamai KSD approach starts from an appreciation of the WAF as one of the most complex web security solutions available to organizations today. With a wide range of required security resources and expertise, few organizations have the capability to deploy and manage a WAF effectively on their own. The KRS is the base for Akamai's WAF solution, increasing accuracy and visibility into attacks as they occur.

3.2 Web Application Firewall (WAF)

A WAF is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. The KSD is an inline implementation of a WAF, sitting in the middle of the HTTP conversation between users and a web application. The WAF inspects HTTP traffic passing through it for any attacks as defined by a list of rules.

3.3 Kona Rule Set (KRS)

Akamai KSD service uses a proprietary rule set named the KRS. The KRS employs a small number of flexible rules in conjunction with an anomaly scoring model to address the design principles of improved accuracy and visibility into attacks. Akamai designed the underlying signatures for every rule to detect different attributes shared by multiple vulnerabilities, rather than the specific vulnerabilities themselves. Because every rule inspects for attributes that are common across multiple vulnerabilities, KRS has a higher likelihood of catching new attack permutations with existing rules. KRS augments its WAF rules with an anomaly detection capability that provides context around individual rule triggers.

3.4 Client Reputation

Client Reputation is an optional module that augments Akamai KSD service with an additional layer of defense using behavioral analysis. While KSD identifies individual malicious HTTP requests, Client Reputation identifies clients at higher risk of issuing those requests. Client Reputation provides a simple mechanism for individual organizations to leverage Akamai's visibility into the actions of 40 million unique IP addresses on a daily basis and hundreds of millions monthly.