ICSA Labs
Web Application Firewalls (WAF) Certification Testing Report
WAF – Criteria Version 2.1

A10 Networks Inc.

A10 Networks AX and Thunder Platform Family

January 17, 2017

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

WAFX–A10NETWORK-2017-0117-01

Table of Contents

A10 Networks Inc.
Web Application Firewalls Certification Testing Report
WAF – Criteria Version 2.1

Executive Summary

Introduction

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 20 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

ICSA Labs manages and facilitates technology consortia that focus on emerging, well-defined technologies. The consortia provide for information exchanges among industry leading developers, and for the development of product testing and certification programs and standards. For more information about ICSA Labs, please visit www.icsalabs.com.

Customer Provided Product Overview

The A10 AX™ and Thunder™ Series is A10 Networks' product family delivering high performance application networking and security solutions, integrating expanded system resources to support future feature needs, and offering our broadest array of physical, virtual and hybrid form factors.

Scope of Assessment

ICSA Labs Web Application Firewalls (WAF) certification program test and certify products that implement security policy enforcement for the protection of HTTP and HTTPS Web-based applications. In conjunction with ongoing efforts in the industry to classify and categorize application security issues and mitigate potential vulnerabilities, the Web Application Firewall certification criteria was developed to provide security managers, application developers and others deploying web based applications with confidence in the products that secure vital application services from exploitation or attack.

Summary of Findings

The Candidate WAF Product has met all of the WAF criteria elements and therefore has attained ICSA Labs WAF Certification. The Candidate WAF Product will remain continuously deployed at ICSA Labs for the length of the testing contract and will be periodically checked as new attacks and vulnerabilities are discovered. In the event that the Candidate WAF Product is found susceptible to new attacks or vulnerabilities during a check, ICSA Labs will work with the vendor to resolve the problems in order for the Candidate WAF Product to maintain its ICSA Labs WAF Certification.

Certification Maintenance

The Candidate WAF Product, like all products and product groups that are granted ICSA Labs WAF Certification, will remain certified on this and future released versions of the product for the length of the testing contract. Future versions will be certified since the product is continuously deployed at ICSA Labs and subjected to periodic spot-checks on the most current product version.

Three circumstances will cause the Candidate WAF Product to have its ICSA Labs WAF Certification revoked:

1. The Candidate WAF Product vendor withdraws from the ICSA Labs WAF Certification Program.
2. The product fails a periodic spot-check and The Candidate WAF Product vendor subsequently fails to provide an adequate fix within a prescribed length of time.
3. The product fails to meet the next full test cycle against the current version of the criteria.

Candidate WAF Product Components

Introduction

The term Candidate WAF Product refers to the complete system submitted by the vendor for certification testing including all documentation, hardware, firmware, software, host operating systems, and management systems. Common network services such as Syslog, DNS, NTP, etc. are provided by ICSA Labs and are not considered part of the Candidate WAF Product.

Hardware

- AX-3400S

Software

Testing began and was successfully completed with version 4.0.3-P1 build 22.

Product Family Description

This section lists the members of the certified product family. A representative set of models was submitted for testing and listed in the Hardware section above. In order to submit a family of products for certification, the vendor must attest that:

- The vendor designs and maintains control over the entire set of hardware, firmware, and software for each member of the product family.
- The vendor software, including but not limited to the functional software and the operating system software, is uniform across the product family.
- The management interface(s) for the members of the product family are uniform and completely consistent.
- Each member in the product family has an equivalent set of functionality.
- The functional, integration, and regression testing conducted by the vendor is uniform and consistent across the product family.

Product Family Members

- TH-vThunder
- TH-1030S
- TH-3030S
- TH-3040S
- TH-3230S
- TH-3430S
- TH-4430S
- TH-4440S
- TH-5330S
- TH-5440S
- TH-5840S
- TH-6430S
- TH-6440S
- TH-6630S
- TH-7440S
- AX-3400S
- AX-5630S
- TH-Baremetal-xxx-ADC

Documentation

To satisfy documentation requirements, A10 Networks Inc. provided ICSA Labs with the following documents in order to assist in the installation, configuration, and administration of the Candidate WAF Product:

- ACOS 4.1.0-P7 Web Application Firewall Reference for A10 Thunder™ Series and AX™ Series 17 November 2016

Introduction

Web Application Firewall products can be configured different ways; therefore, ICSA Labs may face many configuration related decisions before and after installing the Candidate WAF Product. During testing, ICSA Labs attempted to exploit the Candidate WAF Product and its protection of services, so configuration decisions were made to prevent exploitation.

Candidate WAF Product Configuration

ICSA Labs installed and configured the Candidate WAF Product following the vendor's supplied documentation. For the purposes of this testing, the Candidate WAF Product is assumed to be deployed in a firewalled DMZ. Any special configuration or deviations from the documentation that were necessary to execute a test or meet a requirement are documented in this section.

The Candidate WAF Product was configured in reverse proxy mode.

Documentation

Introduction

The Candidate WAF Product documentation should be accurate and applicable to the version tested in providing appropriate guidance for installation, administration, among other information.

Results

ICSA Labs determined the Candidate WAF Product documentation provided adequate and accurate guidance throughout testing for installation and administration.

The Candidate WAF Product met all documentation requirements. No violations were found in this area throughout testing.

Functional and Vulnerability Testing

Introduction

Once configured to enforce a security policy the Candidate WAF Product should properly permit and protect the services allowed by that policy while maintaining the integrity and confidentiality of the data. In this case, "properly" means that the service functions correctly. Confidentiality includes the masking of the internal application structure as well as information displayed to the user of the protected website.

During security testing, ICSA Labs used commercial, in-house, and freely available testing tools to attack and probe the Candidate WAF Product. ICSA Labs used these tools to attempt to defeat or circumvent the security policy enforced by the Candidate WAF Product or exploit the product itself. The attacks include Denial-of-Service, buffer overflow, cross site scripting (XSS), cross site request forgery (CSRF), improper input validation, session mismanagement, information leakage, and other vulnerability testing.

Since there is overlap between functional and vulnerability testing, the results of both phases of testing are presented here.

Results

The Candidate WAF Product was not susceptible to the attacks targeting the product or the intended services. The Candidate WAF Product allowed the services to function as expected while maintaining the integrity and confidentiality of the data.

The Candidate WAF Product met all functional and vulnerability requirements. No violations were found in this area throughout testing.

Logging

Introduction

The Candidate WAF Product is required to provide an extensive logging capability. In practice, this degree of logging may not be enabled at all times or by default; however, the capability must exist on Candidate WAF Product in the event that detailed logging is needed.

ICSA Labs tested the logging functionality provided by the Candidate WAF Product ensuring that it has the ability to capture and present the required system and network event information to audit security related events. ICSA Labs either configured the local logging mechanism or a remote logging mechanism such as syslog. For all logged events ICSA Labs verified that all required log data were recorded.

Results

The Candidate WAF Product has the ability to store logs on either the product itself or send the logs to a host. The Candidate WAF Product was configured to send log messages to a private host via syslog.

The following log example is of a denied HTTP request that was taken from a blacklist policy match:

```
CEF:1|A10|AX3400|4.0.3-P1|WAF|Jan.16.2017.10:03:32|uri-blist-
check|6|src=205.160.130.66.spt=40541.dst=205.160.130.7.dpt=80.hst="mus
icstore.ax3400.prop".cs1=musicStore.cs2=1707155848e3a527.act=deny.md=a
ctive.svc=http.req="GET./siteinfo.php.HTTP/1.1".0.msg="Blacklist.match
!.URI./siteinfo.php.matches.siteinfo".
```

The Candidate WAF Product met all logging requirements. No violations were found in this area throughout testing.

Administration

Introduction

Web application firewall products often have more than a single method by which administration is possible. Whether the product can be administered remotely using vendor provided administration software, from a web browser based interface, via some non-networked connection such as a serial port, or some other means, authentication must be possible before access to administrative functions is granted. ICSA Labs tested not only that authentication mechanisms existed but also that they could not be bypassed and that the remote administration traffic was encrypted and provided session controls.

Results

The Candidate WAF Product was remotely administered from the private network using the available web-based GUI via HTTPS. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful. The remote administration session controls functioned as expected.

The Candidate WAF Product met all administration requirements. No violations were found in this area throughout testing.

Persistence

Introduction

Power outages, electrical storms, and inadvertent power losses should not cause the Candidate WAF Product to lose valuable information such as the remote administration configuration, security policy being enforced, log data, time and date, and authentication data. This section documents the findings of ICSA Labs testing of the Candidate WAF Product against the persistence requirements.

Results

The Candidate WAF Product continued to maintain its configuration, settings, data, and enforcement of the security policy when power was restored following a forced power outage.

The Candidate WAF Product met all persistence requirements. No violations were found in this area throughout testing.

Criteria Violations and Resolutions

Introduction

In the event that ICSA Labs uncovers criteria violations while testing the Candidate WAF Product, the vendor must make repairs before testing can be completed and certification granted. The section that follows documents all criteria violations discovered during testing.

Results

The Candidate WAF Product met all WAF Certification Criteria requirements. No violations were found throughout testing.

Testing Information

This report is issued by the authority of the Managing Director, ICSA Labs. Tests are done under normal operating conditions.

Lab Report Date

January 17, 2017

Please visit www.icsalabs.com for the most current information about this and other products.

Test Location

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

Product Developer's Headquarters

A10 Networks, Inc.
3 West Plumeria Drive
San Jose, CA 95134

This test is accredited under ICSA Labs' ISO/IEC 17025 accreditation issued by ANSI-ASQ National Accreditation Board. Refer to certificate and scope of accreditation number AT – 1423.