Web Application Firewall

Certification Testing Report

Citrix Systems, Inc.
Citrix ADC WAF 14020

ICSA Labs Web Application Firewall Certification Testing Criteria v.2.1

May 24, 2021

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

Table of Contents

Executive Summary

Introduction

The goal of ICSA Labs certification testing is to significantly increase user and enterprise trust in information security products and solutions. For more than 30 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 security, compliance and performance.

Product Overview

Citrix ADC WAF 14020 is a comprehensive web application security solution that blocks known and unknown attacks against web and web services applications. Citrix ADC WAF 14020 enforces a hybrid security model that permits only correct application behavior and efficiently scans and protects known and unknown application vulnerabilities. It analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications.

Scope of Assessment

In ICSA Labs Web Application Firewall (WAF) security certification testing, ICSA Labs determines through a mix of hands on and automated testing whether or not the security vendor's product properly implements security policy enforcement for the protection of HTTP and HTTPS web-based applications. Products are commonly tested against the ICSA Labs Web Application Firewall Certification Criteria. This WAF testing criteria standard was developed in conjunction with ongoing efforts in the WAF industry to provide security managers, application developers and others deploying web based applications with confidence in the products organizations use to secure vital web application services from attack and exploitation over the Internet.

Summary of Findings

Following recent security testing, ICSA Labs confirms that the Citrix ADC WAF 14020 met all of the requirements in the ICSA Labs Web Application Firewall (WAF) testing criteria. As a result of successful security testing the Citrix ADC WAF 14020 retained ICSA Labs WAF Security Certification.

Continuous Deployment and Spot Checks

The tested product will remain continuously deployed at ICSA Labs for the length of the testing contract. If and as relevant new attacks and vulnerabilities are discovered, the deployed WAF model will be periodically checked that it is providing the requisite protection. In the event that the WAF product is found susceptible to new attacks or vulnerabilities during a check, ICSA Labs will work with the security product vendor to resolve the problems in order for the WAF product to maintain its ICSA Labs WAF Security Certification.

Certification Maintenance

This WAF product, like all WAFs and families of related WAF models 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, barring any criteria-related shortcomings discovered during periodic spot checks.

WAF Product Components

Hardware

For the recently completed ICSA Labs web application firewall (WAF) test cycle, Citrix Systems provided the following WAF model for security certification testing:

- Citrix ADC WAF 14020 (herein referred to as ADC 14020)

Software

Testing began with and successfully completed with version 13.0.41.20.

Documentation

To satisfy documentation requirements, Citrix provided ICSA Labs with the following resource in order to assist in the installation, configuration, and administration of their WAF product:

- Citrix Product Documentation for Citrix ADC 13.0.41.20

Installation and Configuration

Web Application Firewall products can be configured different ways; therefore, ICSA Labs typically faces many configuration related decisions before product installation as well as afterward. During testing, ICSA Labs attempted to exploit the WAF product and its protection of services, therefore configuration decisions were made to prevent such exploitation.

ICSA Labs installed and configured the product following the vendor's supplied documentation. For the purposes of this testing, ICSA Labs assumes that the WAF product would 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 product was configured in reverse web proxy mode for inbound connections.

Documentation

Expectation

The WAF product documentation should be accurate and applicable to the version tested while providing appropriate guidance for installation, administration and other related information.

Results

ICSA Labs determined that in terms of installation and administration, the ADC 14020 documentation was adequate and accurate.

The ADC 14020 met all documentation requirements. No violations were found in this area throughout testing.

Functional and Vulnerability Testing

Expectation

Once configured to enforce a security policy the security vendor's 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 WAF product. ICSA Labs used these tools to attempt to defeat or circumvent the security policy being enforced by the WAF product. In some cases the tools were used in an attempt to 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 web application threats.

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

Results

The ADC 14020 model tested were not susceptible to attacks targeting the product. In addition, the services being targeted were similarly unharmed. In fact, the Citrix ADC WAF 14020 allowed the applications to function as expected while maintaining the integrity and confidentiality of the data.

The ADC 14020 model therefore met all functional and security requirements. No violations were found in this area throughout testing.

Logging

Expectation

The 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 tested WAF products in the event that detailed logging is needed by an organization.

ICSA Labs tested the logging functionality provided by the 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 was recorded.

Results

The ADC 14020 has the ability to either store logs on the product itself or to send any logged data to a remote device. In testing, log data was collected both locally and from syslog.

The following log message taken from syslog depicts a manual system time change as written in a persistent log on the ADC 14020:

```
May 19 12:23:00 <local0.info> citrix-nsmpx8200 nsfsyncd: System time was set back at
least 25226 seconds (Wed May 19 19:23:26 2021 to Wed May 19 12:23:00 2021)
```

The ADC 14020 models therefore met all logging requirements. No violations were found in this area throughout testing.

Administration

Expectation

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. In addition ICSA Labs tested to determine whether remote administration traffic was encrypted and provided session controls.

Results

The ADC 14020 was remotely administered from a private network using the available web-based GUI via HTTPS as well as the CLI via a serial connection. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful. The remote administration session controls functioned as expected.

The ADC 14020 model tested therefore met all administration requirements. No violations were found in this area throughout testing.

Persistence

Expectation

Power outages, electrical storms, and inadvertent power losses should not cause the 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 WAF product against the persistence requirements.

Results

When power was restored following a forced power outage, the ADC 14020 continued to maintain its configuration, settings, and data while enforcing the appropriate, configured security policy.

The ADC 14020 therefore 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-related shortcomings while testing the WAF product, it is incumbent upon the security vendor to make repairs before testing can be completed and certification granted or retained. The section that follows documents any and all criteria violations found by ICSA Labs during testing.

Results

The ADC 14020 met all of the ICSA Labs Web Application Firewall Certification Criteria requirements. There were no violations discovered during this test cycle.

ICSA Labs Certified Web Application Firewalls

Because the Citrix ADC WAF 14020 passed all ICSA Labs web application firewall security tests and as the tested product met the entire set of testing criteria requirements, ICSA Labs is pleased to confirm that the Citrix ADC WAF 14020 has retained ICSA Labs Web Application Firewall Certification.

Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.

Darren Hartman

Darren Hartman, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 30 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.

www.icsalabs.com

Citrix Systems, Inc.

Citrix (NASDAQ: CTXS) builds the secure, unified digital workspace technology that helps organizations unlock human potential and deliver a consistent workspace experience wherever work needs to get done. With Citrix, users get a seamless work experience and IT has a unified platform to secure, manage, and monitor diverse technologies in complex cloud environments.

www.citrix.com