Spikes Security – Isla® Browser Isolation System

Prepared for Spikes Security

April 8, 2015

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

Table of Contents

Executive Summary

Spikes Security asked ICSA Labs, an Independent Division of Verizon to evaluate the Spike's Isla® Browser Isolation System. The goal of this engagement was to evaluate the Isla® Browser Isolation System's effectiveness in protecting users from web borne malware.

As a result of the testing, ICSA Labs did not observe any web based malware being delivered to the Isla Client system.

Spikes Security – Isla® Browser Isolation System Overview

The Isla solution consists of multiple appliance configurations that scale to support any number of users working inside the enterprise. In addition, Isla appliances can be deployed in a public, private, or hybrid cloud configuration to support users working outside the corporate network. The Isla client viewer application – available for Windows, OSX and Linux platforms - connects to appliances to safely access web content without fear of any malware attacks.

ICSA Labs evaluated version 1.1.20 of the Isla® Browser Isolation System.

Evaluation Criteria

Functional Security –
ICSA Labs tested that the product performs its intended security operation to protect the client web browser access to the internet:

- Protects the client from web browser-borne malware
- When accessing secure web sites:
    - Supports TLS v1.2 protocol and AES256-SHA256 cipher suite
    - Properly validates server certificates and alerts the client when a certificate cannot be validated
    - Protects the client's private web browser data

Platform Security
ICSA Labs tested that the product is secure as deployed per the administrative guidance, verifying that the product:

- Is not vulnerable to remotely executable exploits known within the information security community
- Is not rendered inoperable to trivial denial-of-service attacks
- Does not introduce vulnerabilities or security-degrading mistakes
- Does not leak data between virtual sessions
- Provides secure remote administration such that:
    - remote administration traffic is protected using standards based cryptography
    - the product does not allow unauthorized access to administrative functions
- Provides secure communications between clients and the appliance such that:
    - traffic is protected using standards based cryptography
    - the product does not allow unauthorized access to its services

Logging

- ICSA Labs tested that product provides adequate logging to audit the following specific events:

- A successful or failed administrative authentication
- A successful or failed client authentication

Initial Setup

Spikes Security provided ICSA Labs with the Isla controller and appliance. For testing purposes, the controller and appliance were deployed within the same subnet as the client system running the Isla browser application. The controller and appliance arrived preconfigured for testing and ready to connect to the network. ICSA Labs elected to install the Isla browser application on a Windows XP SP3 client system without any other security protection software, configurations, or updates to keep the system vulnerable to malware during the malicious URL testing. Monitoring software was installed on the client system to make comparison snapshots and monitor for malware infection changes. The network traffic of the controller, appliance, and client system was monitored and analyzed throughout testing to help confirm the results.

Evaluation Results

Protects the client from web browser-borne malware
ICSA Labs captured live traffic of a vulnerable system accessing malicious URLs. ICSA Labs then attempted to send the captured attacks through the Isla appliance and deliver the malware to the Isla client. Throughout the malicious URL testing, network traffic was monitored to confirm that the malicious payload was sent. The Isla client system remained unchanged and showed no signs of an attack or infection. There was no evidence that the Isla appliance acted on, execute or deliver, any malicious payload.

When accessing secure web sites: Supports TLS v1.2 protocol and AES256-SHA256 cipher suites
Using a secure web server to test the client/server SSL/TLS negotiations, ICSA Labs confirmed the Isla appliance supported TLS v1.2 AES256-SHA256 connections and did not propose weak cipher suites in the TLS Client Hello messages.

When accessing secure web sites: Properly validates server certificates and alerts the client when a certificate cannot be validated
ICSA Labs configured a secure web server with a valid server certificate, an expired server certificate, a server certificate that the Common Name did not match the server host name in the URL, and a server certificate that was not properly signed by the trusted Certification Authority. Testing showed that the Isla appliance properly rejected the connections when presented with certificates that were not valid. However, when tested with a revoked server certificate, the appliance did allow the connection and did not notify the client of the revocation status.

When accessing secure web sites: Protects the client's private web browser data
The Isla system did not appear to support caching user's private information within the Isla browser. The information, such as website authentication credentials and form data, was not persistent from previous browser sessions.

Is not vulnerable to remotely executable exploits know within the information security community; does not introduce vulnerabilities or security-grading mistakes
ICSA Labs' security assessment tested for but did not reveal any exploitable remote vulnerability on the Isla controller or appliance. Access to the CLI indicated that Debian 7.8 wheezy and OpenSSL package 1.0.1e-2+deb7u16 were installed. These were the latest releases and addressed many security issues, including the Bash vulnerability

Is not rendered inoperable to trivial denial-of-service attacks
ICSA Labs attacked the Isla appliance with a SYN-flood targeting open client session ports. This had an adverse effect on the communication responses between the appliance and the Isla browsers using the ports. Because of the attack, client sessions that had been terminated appeared to still be in use on the appliance.

Does not leak data between virtual sessions
ICSA Labs' review of the Isla appliance did not uncover any issues regarding data leaking between virtual sessions. It should be noted that ICSA Labs' access to the Isla system was based on non-privileged accounts, limiting the extent of searching for indications of compromise.

Provides secure remote administration such that: Remote administration traffic is protected using standards based cryptography
The Isla controller's remote administration through the Web UI was protected using TLS v1.2 DHE-RSA-AES128-SHA256. Accessing the controller and appliance CLI over an SSH connection was protected using AES256-SHA2-256.

Provides secure remote administration such that: The product does not allow unauthorized access to administrative functions
ICSA Labs confirmed that accessing the administrative functions required proper authentication.

Provides secure communications between clients and the appliance such that: Traffic is protected using standards based cryptography
ICSA Labs could not verify that standards based cryptography was used for communications between the Isla clients and appliance. Spikes Security stated that the communication traffic between the Isla appliance and the client system is a proprietary protocol wrapped in AES256-bit symmetric encryption. ICSA Labs confirmed that the data did not disclose protected information.

Provides secure communications between clients and the appliance such that: The product does not allow unauthorized access to its services
The Isla browser required proper authentication with the controller initially to register the client system after installation. Once the system was registered, the browser was able to access the Internet through the appliance without any further authentication. Authentication to the controller was required each time the user's bookmarks and history were accessed within the browser. ICSA Labs determined that by copying the Isla application data files from a registered system onto an unregistered system, the unregistered system was able to bypass the initial registration authentication process and access the Internet as the registered user.

Logging: A successful or failed administrative authentication
The Isla controller provided logs for successful and failed Web UI authentications.

Logging: A successful or failed client authentication
The Isla controller provided logs for successful and failed client authentications.

Testing Notes

We experienced some stability issues with the pre-release version of the Isla software that was provided to us for testing. However the company subsequently provided a later version of the software which corrected this problem.

Appendix A

Malicious URL's used for testing engagement. Note that the http string was changed to prevent accidental clicking of a malicious link.

URLs:
hxxp://archoncybertech.com.au/clienthosting/acatrees/testimonials.html

hxxp://archoncybertech.com.au/clienthosting/acatrees/testimonials.html

hxxp://bbs.pxecn.com/forum.php?mod=attachment&aid=Nzc5OTl8MWQ0Mjc4MTV8MTM2OTgyMTc0NnwxMTE5OHwxMDY1NjU=

hxxp://bbs.pxecn.com/forum.php?mod=attachment&aid=Nzc5OTl8MWQ0Mjc4MTV8MTM2OTgyMTc0NnwxMTE5OHwxMDY1NjU=

hxxp://bibliotecacenamec.org.ve/logo.gif?164cf=456715

hxxp://bibliotecacenamec.org.ve/logo.gif?164cf=456715

hxxp://blog.pixelbomber.net/?p=18

hxxp://cdn3.partners-serving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=20322

hxxp://cdn3.partners-serving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=20322

hxxp://cdn3.partners-serving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=31964

hxxp://cdn3.partners-serving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=31964

hxxp://cdn3.partners-serving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=4518

hxxp://cdn3.partners-serving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=4518

hxxp://cdn3.partnerserving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=18684

hxxp://cdn3.partnerserving.com/toolbar/pub/66920/6787/download/HomeTab.exe?rnd=18684

hxxp://chinamv.net.cn

hxxp://chinamv.net.cn

hxxp://consonchina.cn/download

hxxp://csskafa.blogspot.ca

hxxp://dailyreport.cffy88.com/Notifica.zip?AwOtRx=lanebarberis+at+li%2Ffile%2F6a38368ca3cdc5d1c1b6f23528778377%3Ffid%3D237824064-250528-1208529444

hxxp://dailyreport.cffy88.com/Notifica.zip?AwOtRx=lanebarberis+at+li%2Ffile%2F6a38368ca3cdc5d1c1b6f23528778377%3Ffid%3D237824064-250528-1208529444

hxxp://DDE.DE.RESOURCE-EFILES-DRIVE.COM/1/965/ct9652401/d8b382a91d48496ca87690f22678ef6a/downloads/prod/smallstub1.3.9.0.140504.01/15-02-28-17.18.07.828/stardoll.exe

hxxp://DDE.DE.RESOURCE-EFILES-DRIVE.COM/1/965/ct9652401/d8b382a91d48496ca87690f22678ef6a/downloads/prod/smallstub1.3.9.0.140504.01/15-02-28-17.18.07.828/stardoll.exe

hxxp://DDE.DE.RESOURCE-EFILES-DRIVE.COM/45/873/ct8732245/8ac71ca986564002987411d4e88cb0be/downloads/prod/smallstub1.3.9.0.140504.01/15-02-28-16.36.19.030/icytower.exe

hxxp://DDE.DE.RESOURCE-EFILES-DRIVE.COM/47/412/ct4120647/ff6914cb444e483c864031ba34329d5e/downloads/prod/smallstub1.3.9.0.140504.01/15-03-01-02.22.49.472/stardoll.exe

hxxp://DDE.DE.RESOURCE-EFILES-DRIVE.COM/47/412/ct4120647/ff6914cb444e483c864031ba34329d5e/downloads/prod/smallstub1.3.9.0.140504.01/15-03-01-02.22.49.472/stardoll.exe

hxxp://DDE.DE.RESOURCE-EFILES-DRIVE.COM/66/637/ct6375566/5b2ebe154b524b83a333ad1da7b378b5/downloads/prod/smallstub1.3.9.0.140504.01/15-02-28-20.20.42.390/etvonline.exe

hxxp://DDE.DE.RESOURCE-EFILES-DRIVE.COM/66/637/ct6375566/5b2ebe154b524b83a333ad1da7b378b5/downloads/prod/smallstub1.3.9.0.140504.01/15-02-28-20.20.42.390/etvonline.exe

hxxp://DDE.S.AONDEMAND-ABOUT.COM/62/220/ct2204562/f349938c7be548efaa3a67c5cc11ae83/downloads/prod/smallstub1.3.9.0.140504.01/15-02-28-21.09.01.121/autocaddrawingviewer.exe

hxxp://DDE.S.AONDEMAND-ABOUT.COM/62/220/ct2204562/f349938c7be548efaa3a67c5cc11ae83/downloads/prod/smallstub1.3.9.0.140504.01/15-02-28-21.09.01.121/autocaddrawingviewer.exe

hxxp://DDE.S.DDIRECTDOWNLOAD-ABOUT.COM/32/805/ct8051332/948d71e82d9147abb6ebd73f8e4fbebe/downloads/prod/dde1.4.0.5.150121.02/15-02-28-18.18.07.952/incredimail.exe?filename=incredimail_tsa1xlg8t.exe

hxxp://DDE.S.DDIRECTDOWNLOAD-ABOUT.COM/32/805/ct8051332/948d71e82d9147abb6ebd73f8e4fbebe/downloads/prod/dde1.4.0.5.150121.02/15-02-28-18.18.07.952/incredimail.exe?filename=incredimail_tsa1xlg8t.exe

hxxp://DDE.S.DDIRECTDOWNLOAD-ABOUT.COM/32/805/ct8051332/948d71e82d9147abb6ebd73f8e4fbebe/downloads/prod/dde1.4.0.5.150121.02/15-02-28-18.18.07.952/incredimail.exe?filename=incredimail_tsv3gpwd7.exe

hxxp://DDE.S.DDIRECTDOWNLOAD-ABOUT.COM/32/805/ct8051332/948d71e82d9147abb6ebd73f8e4fbebe/downloads/prod/dde1.4.0.5.150121.02/15-02-28-18.18.07.952/incredimail.exe?filename=incredimail_tsv3gpwd7.exe

hxxp://dentalsouthchina.com/product_info.asp?p_id=2736&sortid=19&sortname=%C6%E4%CB%FB

hxxp://dentalsouthchina.com/product_info.asp?p_id=2736&sortid=19&sortname=%C6%E4%CB%FB

hxxp://dl.desk1992get.com/n/13127927/MATLAB.exe?secure=1424868624_1de3307ad04bdd93c947896cb7b66fde

hxxp://dl.desk1992get.com/n/13127927/MATLAB.exe?secure=1424868624_1de3307ad04bdd93c947896cb7b66fde

hxxp://dl.desk1992get.com/n/3.2.10/13101715/Bluestacks%20Offline%20Installer.exe

hxxp://dl.desk1992get.com/n/3.2.10/13101715/Bluestacks%20Offline%20Installer.exe

hxxp://DL.DESK1992GET.COM/n/3.2.131/10227646/smart+movingmod+5.exe

hxxp://DL.DESK1992GET.COM/n/3.2.131/10227646/smart+movingmod+5.exe

hxxp://DL.DESK1992GET.COM/n/3.2.131/13944315/stellar_phoenix_excel_recovery_4.exe

hxxp://DL.DESK1992GET.COM/n/3.2.131/13944315/stellar_phoenix_excel_recovery_4.exe

hxxp://dl.getdesk1994.com/n/15881535/Fluvore_Downloader.exe

hxxp://dl.getdesk1994.com/n/15881535/Fluvore_Downloader.exe

hxxp://DL.POCODOCTOR.COM/n/3.2.131/11736878/dj+music+mixer.exe

hxxp://DL.POCODOCTOR.COM/n/3.2.131/11736878/dj+music+mixer.exe

hxxp://DL.POCODOCTOR.COM/n/3.2.131/13726914/winrar.exe

hxxp://dl.pocomissus.com/n/11975528/7Zip.exe?secure=1424988631_82dd0d6
1ecbc3fa2f9614096b836623a

hxxp://dl.pocomissus.com/n/3.2.96/12744920/Showbox%20Installer.exe?

hxxp://dl.pocomissus.com/n/3.2.96/12744920/Showbox%20Installer.exe?

hxxp://dl.tutofourpc.com/download/udp/majt4pc.exe?jUrMqP9yIX5AJhR+RHf8
uLq8Lu0hgMAOTbpyelUXKDsEAPmeeRrW4+hfGX8fDFbEoHAU7xWKnoTeflbhPsftJhz590
9FTnhG58sYiX3HBAv4gnd+XQjnEg==

hxxp://dl.tutofourpc.com/download/udp/majt4pc.exe?jUrMqP9yIX5AJhR+RHf8
uLq8Lu0hgMAOTbpyelUXKDsEAPmeeRrW4+hfGX8fDFbEoHAU7xWKnoTeflbhPsftJhz590
9FTnhG58sYiX3HBAv4gnd+XQjnEg==

hxxp://dl4.getz.tv/setup/ZonaWebSetup.exe?pid=60&url=hxxp%3A%2F%2Fdl.2
4video.net%2F3c779dff37c034a019b380192c6d37c4%2F1242%2F1242626%2Frelak
satsiya_po_russki.mp4&title=%D0%A0%D0%B5%D0%BB%D0%B0%D0%BA%D1%81%D0%B0
%D1%86%D0%B8%D1%8F+%D0%BF%D0%BE+%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%B8&c
over=hxxp%3A%2F%2Fimg3.24video.net%2F1242%2F1242626%2Fframe00000.jpg&a
utoplay=true&adult=true

hxxp://dmpattenonline.com/?page_id=69

hxxp://down.reaboo.com/setup/all/xk/V1.0.2.574/db/xiakan_xk_db2.exe

hxxp://down.youbo.cc/setup/all/cpa/V4.7.1.104/K/Youbo_K154626.exe

hxxp://down.youbo.cc/setup/all/cpa/V4.7.1.104/K/Youbo_K154626.exe

hxxp://down3.15111358088.cn/adfgdg-1014-
881454(???
??
??
??
??
??
??
??
??
??

??
??
??
??
??
??
??
??
??
??????????????????????????????????

hxxp://down3.15111358088.cn/adfgdg-1014-
881454(??
??
??
??
??
??
??
??
??
??
??
??
??
??
??
??
??
??
??????????????????????????????????

hxxp://download2v.freesoftstore2.com/installers/out/012030120401205/pi
id-
547fd1ebb6aca7.60233462/on/2/freesoftstorecom/english/revenue/msie/ado
be_flash_player/d/275876e34cf609db118f3d84b799a790/ici/na/na/installer
_adobe_flash_player_English.exe