Malware Monitoring Report

Indusface

http://demo1.indussecure.com/

Confidential

Scan Date: 2023-09-26

Scope

Malware Monitoring for URL http://demo1.indussecure.com/

Limitations

1. The entire test was carried out with no prior knowledge of the systems and applications.
2. All test were carried out without any known credentials to systems and applications.
3. Indusface WAS does not allowed to carry out any DoS attacks or to run any exploits which can affect systems availability.

Confidentiality

This document contains sensitive and/or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained with in this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, Indusface WAS, assumes no liability for the completeness, use of, or conclusions drawn from such data.

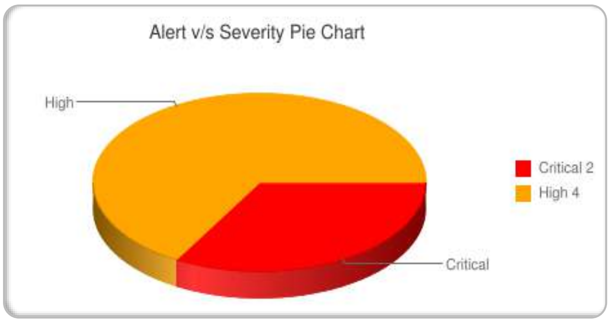
Disclaimer

This, or any other, Security Audit cannot and does not guarantee security. Indusface WAS makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that Indusface WAS shall be held harmless in any event. Indusface WAS makes this information available solely under its Terms of Service Agreement published at was.indusface.com.

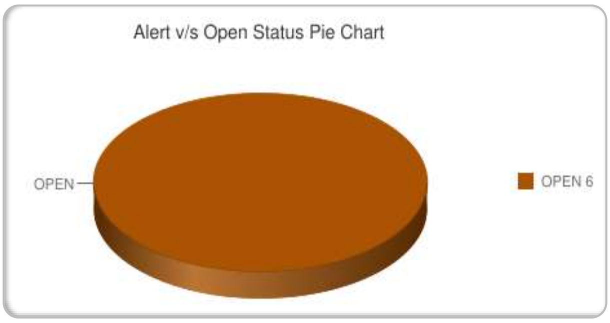
Executive Summary

Total number of alert(s) identified are 6

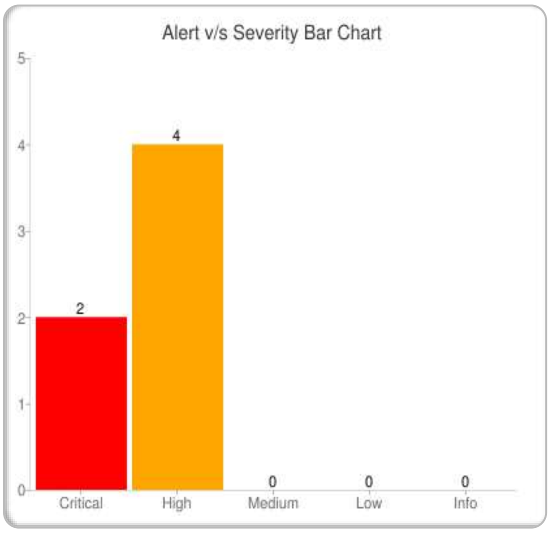
Alert v/s Severity Pie Chart



Alert v/s Open Status Pie Chart



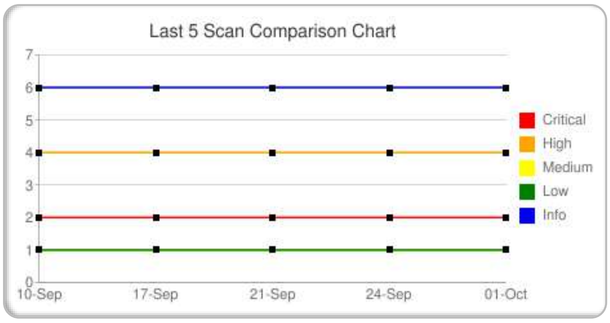
Alert v/s Severity Bar Chart



Alert Summary

Severity	Total
Critical	2
High	4
Medium	0
Low	0
Info	0

Comparison Chart



Comparison Summary

Severity	10 Sep	17 Sep	21 Sep	24 Sep	01 Oct
Critical	2	2	2	2	2
High	4	4	4	4	4
Medium	1	1	1	1	1
Low	1	1	1	1	1
Info	6	6	6	6	6

Alert Details

Title	Total
Malware Identified	1
Website Blacklisted	1
Foreign Link Blacklisted	1
Possible Defacement Detected	1
Suspicious Redirection Detected	1
Suspicious URL	1

URL Blacklist Status

Google Blacklist	✓	SAFE
Google Malware	✓	SAFE
Norton Safe Web	✓	SAFE
Mcafee	✓	SAFE
PhishTank	✓	SAFE
Bing	✓	SAFE
Yahoo	✓	SAFE

Alerts

Alert ID:785430 Found on: 2023-09-26 🟥 Severity: Critical

Website Blacklisted

Open Status: OPEN **First Found:** 2023-10-17

Link Placed On: http://demo1.indussecure.com/
Affected URL: http://demo1.indussecure.com/

Detail:

Your website is blacklisted by one or more below listed blacklisting databases.

- Google Malware Blacklisting Database
- Google Phishing Database
- Norton Blacklisting Database
- McAfee Blacklisting Database
- PhishTank Blacklisting Database
- Bing Search Blacklisting Database
- Yahoo Search Blacklisting Database

Solution:

IndusGuard has detected that your website is blacklisted. To remove your website from blacklisting database, please identify and clean the suspected content and ask for review which has blacklisted your website.

Result:

```
McAfee Blacklisted
```

Alert ID:785612	Found on: 2023-09-26	🟥 Severity: Critical

Malware Identified

Open Status: OPEN **First Found:** 2017-07-10

Link Placed On: http://demo1.indussecure.com/
Affected URL: http://demo1.indussecure.com/

Detail:

The requested URL is MALWARE INFECTED. The URL contains malicious software which can be designed to disrupt or deny the specific operation, gather information which might lead to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviours. These kinds of activities can cause serious security problems or resource problems to this website or to the users of this website.

Solution:

IndusGuard has detected malware on Internal URL. Please remove the malware infected code from URL to safeguard visitors of your website.

Alert ID:786229	Found on: 2023-09-26	🟧 Severity: High

Suspicious URL

Open Status: OPEN **First Found:** 2017-07-24

Link Placed On: http://demo1.indussecure.com/
Affected URL: http://demo1.indussecure.com/china-chine/visa.aspx?lang=eng

Detail:

The requested URL is MALWARE INFECTED. The URL contains malicious software which can be designed to disrupt or deny the specific operation, gather information which might lead to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviours. These kinds of activities can cause serious security problems or resource problems to this website or to the users of this website.

Solution:

IndusGuard has detected malicious activities on external URL. Please remove the malware infected URL from your website to safeguard visitors of your website.

Result:

```
One of resource available on this page is Malware Infected□.
Resource Name : http://purl.org/dc/terms/
Resource URL : http://purl.org/dc/terms/
```

Alert ID:785429	Found on: 2023-09-26	🟧 Severity: High

Foreign Link Blacklisted

Open Status: OPEN **First Found:** 2023-10-17

Link Placed On: http://demo1.indussecure.com/
Affected URL: http://demo1.indussecure.com/

Detail:

The external URL placed on your website is blacklisted by one or more below listed blacklisting databases.

- Google Malware Blacklisting Database
- Google Phishing Database
- Norton Blacklisting Database
- McAfee Blacklisting Database
- PhishTank Blacklisting Database
- Bing Search Blacklisting Database
- Yahoo Search Blacklisting Database

Solution:

IndusGuard has detected that external URL is blacklisted. Please remove the malware infected URL from your website to safeguard visitors of your website.

Result:

```
Google Malware Blacklisted URL found on your website.
```

Alert ID:787457 Found on: 2023-09-26 Severity: High

Possible Defacement Detected

Open Status: OPEN **First Found:** 2017-08-21

Link Placed On: http://demo1.indussecure.com/
Affected URL: http://demo1.indussecure.com/

Detail:

The URL contains suspicious defacement activity. An URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Solution:

IndusGuard has done research on the page and has detected some suspicious changes in code. Please compare below mentioned actual and modified source codes and take appropriate action.

Alert ID:787527 Found on: 2023-09-26 Severity: High

Suspicious Redirection Detected

Open Status: OPEN **First Found:** 2017-08-24

Link Placed On: http://demo1.indussecure.com/
Affected URL: http://demo1.indussecure.com/

Detail:

The URL behaves abnormally when opened with referrer and redirects users to some other host which looks like some suspicious activity. The redirected host may be untrusted or risky, it may create security related issue to users of your website. This kind of redirection may lead to misguide search engines and they may link your website with some other search-results/web sites.

Solution:

Please verify all start-up configuration files for web site, remove all suspicious entries from .htaccess/web.confile file.