b e S E C U R E

SCAN RESULTS

Coralogix PCI scan
January 21, 2019

Coralogix

Revision: 2.0

Vulnerability Report

Table of Contents

Introduction

The 'Coralogix PCI scan' scan has been completed.

You requested a report of the following host(s): coralogix-esapi.coralogix.com, api.coralogix.com.

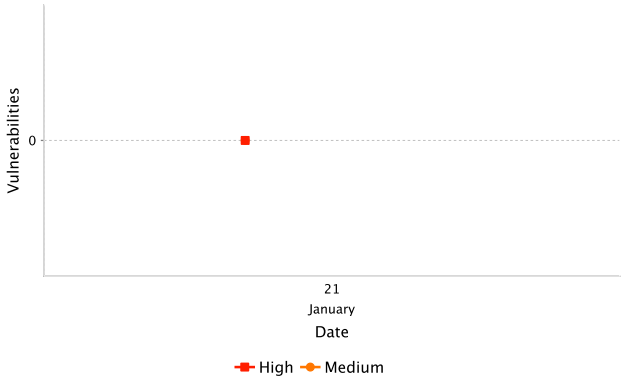
The scan took place on 2019-01-21 12:40:02 (Scan Number: 6).

The 'Possible Vulnerabilities' section of this report lists security holes found during the scan, sorted by risk level. Note that some of these reported vulnerabilities could be 'false alarms' since the hole is never actually exploited during the scan.

Some of what we found is purely informational; It will not help an attacker to gain access, but it will give him information about the local network or hosts. These results appear in the 'Low risk / Intelligence Gathering' section.

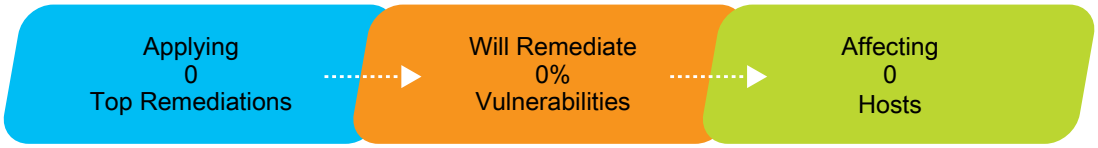
Vulnerability Trend

High and Medium Risk totals discovered on scan 'Coralogix PCI scan' and their change in number over time.



Remediation Focus

Repair the most common security issues on scan 'Coralogix PCI scan' and 0% of its vulnerabilities will be resolved.



Further Information

Download the following additional reports:

- Penetration Test
- Based on PCI-DSS compliance (non-official)
- OWASP
- SOX
- HIPAA
- ISO 27001/2
- CIS (Only relevant if you enabled CIS Compliance scan)
- Remediation
- Differential
- Microsoft Patches

Executive Summary

Vulnerabilities in the report are classified into 3 categories: high, medium or low. This classification is based on industry standards and is endorsed by the major credit card companies. The following is the categories definitions:

High Risk Vulnerability

are defined as being in one or more of the following categories: Backdoors, full Read/ Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords)

Medium Risk Vulnerability

are vulnerabilities that are not categorized as high risk, and belong to one or more of the following categories: Limited Access to files on the host, Directory Browsing and Traversal, Disclosure of Security Mechanisms (Filtering rules and security mechanisms), Denial of service, Unauthorized use of services (e.g. Mail relay).

Low Risk Vulnerability

are those that do not fall in the "high" or "medium" categories. Specifically, those will usually be: Sensitive information gathered on the server's configuration, Informative tests.

Host information - provided by different tests that discover information about the target host, results of those test are not classified as vulnerabilities.

Guessed Platform - Detection of the operation system running on the host, via TCP/IP Stack FingerPrinting, this test is not very accurate, thus it is guessing.

Executive Summary

Top Level Overview					
Scan	Total	High	Medium	Low	Score
Coralogix PCI scan	3	0	0	3	100.00

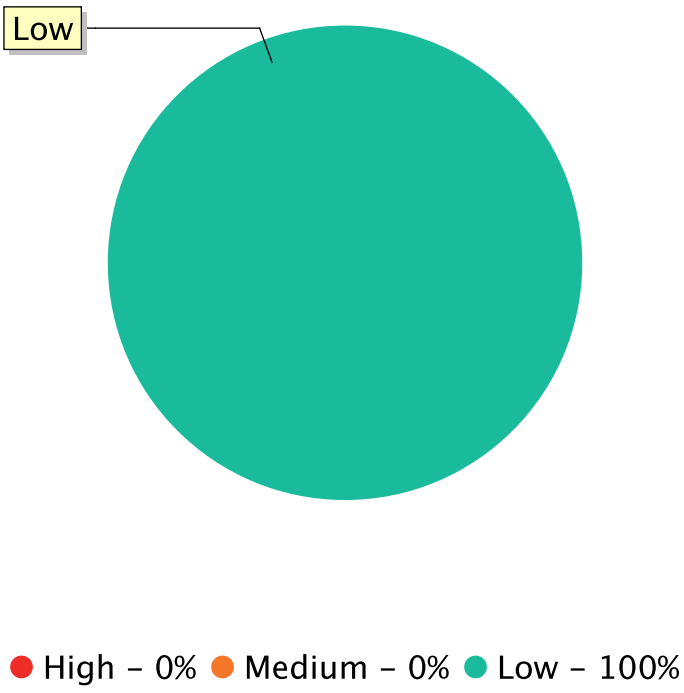
Vulnerabilities by Host and Risk Level					
Host	Total	High	Medium	Low	Score
api.coralogix.com	3	0	0	3	100.00
coralogix-esapi.coralogix.com	0	0	0	0	100.00
Number of host(s): 2					

Vulnerabilities by Service and Risk Level					
Service	Total	High	Medium	Low	Score
https (443/tcp)	3	0	0	3	100.00

Vulnerabilities by Category					
Category	Total	High	Medium	Low	Score
Encryption and Authentication	2	0	0	2	100.00
Web servers	1	0	0	1	100.00

Possible Vulnerabilities

Vulnerabilities Breakdown by Risk



1. SSL VERIFICATION TEST / Encryption and Authentication

Host(s) affected:

api.coralogix.com: https (443/tcp)

Summary:

This test connects to a SSL server, and checks its certificate and the available ciphers. Weak (export version) ciphers are reported as problematic.

api.coralogix.com : https (443/tcp)

Here is the server certificate:
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 6887070034682949483 (0x5f93c9b51083af6b)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
Validity
Not Before: Jan 16 18:59:00 2018 GMT
Not After : Jan 16 11:04:03 2021 GMT
Subject: OU=Domain Control Validated, CN=*.coralogix.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:a7:93:44:0d:e5:44:d5:f2:69:9b:73:21:a0:ef:
68:0d:55:c7:80:78:a8:e3:d1:17:ee:fd:e6:96:38:
50:80:b3:3e:f4:92:70:91:43:a8:b7:1a:c7:0d:a3:
a6:0a:c9:fa:c1:82:6a:5a:36:57:fd:ad:bd:35:f6:
af:19:1e:fe:ac:34:5b:ef:75:76:18:02:6e:06:59:
44:e4:4d:74:05:01:b4:ae:b0:55:7e:1f:a4:1d:ed:
49:57:ff:5f:5e:1d:89:ac:e4:61:7e:93:b7:d2:55:
df:a5:8e:07:f0:e0:f7:56:2c:02:ab:1b:75:21:c9:
7b:ca:24:27:d7:a8:74:21:68:2f:8b:59:ad:50:bc:
f8:2d:a7:da:67:73:f4:ab:18:06:8f:01:84:c9:7d:
6a:b4:79:a3:1c:57:da:b2:f6:da:80:59:ef:fe:72:
a9:72:ad:d5:9d:3a:eb:81:cf:c3:96:80:a0:fe:a3:
86:98:80:47:af:6b:f3:84:48:f6:28:ed:56:21:2b:
b5:cd:ee:d4:9a:6d:60:80:cd:31:be:85:79:2c:71:
d8:2b:28:1e:ba:2d:6a:c5:16:76:ae:63:dc:bc:bd:
ca:62:31:5b:27:d3:98:02:67:93:8d:2d:18:b6:f9:
f0:2d:89:90:56:4d:cb:5a:c9:fe:a7:66:7b:1a:51:

01:c9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 CRL Distribution Points:

Full Name:
URI:http://crl.godaddy.com/gdig2s1-801.crl

X509v3 Certificate Policies:
Policy: 2.16.840.1.114413.1.7.23.1
CPS: http://certificates.godaddy.com/repository/
Policy: 2.23.140.1.2.1

Authority Information Access:
OCSP - URI:http://ocsp.godaddy.com/
CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt

X509v3 Authority Key Identifier:
keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE

X509v3 Subject Alternative Name:
DNS:*.coralogix.com, DNS:coralogix.com
X509v3 Subject Key Identifier:
C3:D6:42:AA:C4:44:39:BE:74:50:5B:66:2C:1C:28:E0:20:FA:16:9F
Signature Algorithm: sha256WithRSAEncryption
3e:e5:e2:77:1f:a5:fd:38:1e:82:02:3c:67:99:f1:33:90:3f:
ec:cd:97:66:c3:98:71:62:b8:d1:d2:ef:17:ab:21:d6:58:6c:
10:2c:ee:f8:f7:d0:98:9e:14:5b:3d:67:d3:ff:5e:1c:f4:d3:
29:f1:87:a1:34:9d:80:56:4b:21:da:43:c3:fd:08:34:f3:c2:
c8:60:a2:39:75:9b:59:a3:23:13:18:da:ce:c4:20:f5:46:dc:
06:0b:43:2e:b2:8a:87:db:9a:10:e6:14:61:2c:71:42:f3:da:
15:38:26:ad:fb:b8:9b:dc:0b:2d:bc:3a:02:b1:fa:fd:98:45:
d2:35:45:a5:2b:f3:a4:53:e1:c3:d3:64:72:bc:78:b2:08:e2:
6c:ee:31:b1:35:7f:91:2e:b4:8d:cb:06:5a:77:02:af:e2:b5:
24:dd:85:20:b0:e1:c0:88:01:7e:50:6b:37:76:40:53:54:79:
c4:0a:b3:a4:9f:2f:e4:95:5c:26:90:28:b0:5d:f9:ee:54:4a:
7f:36:9c:25:26:5a:fc:a5:34:0d:5d:82:c9:34:1b:58:be:f0:
5f:0e:15:cb:d4:c2:45:49:eb:f0:f2:d0:04:19:df:c1:3f:98:

48:4a:f9:22:37:2d:a7:d1:4d:bd:a2:ff:19:4a:d6:6a:8c:84:
dc:5d:9f:a9
This SSLv2 server does not accept SSLv3 connections.
This SSLv2 server also accepts TLSv1 connections.

Possible Solution:

Usage of weak ciphers should be avoided.

Risk: Low

CVSS Score: *

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

TestID: 2804 (Revision: 4, Added: 2003-12-25)

2. SUPPORTED SSL CIPHERS SUITES / Encryption and Authentication

Host(s) affected:

api.coralogix.com: https (443/tcp)

Summary:

This test detects which SSL ciphers are supported by remote service for encrypting communications.

api.coralogix.com : https (443/tcp)

Here is the list of SSL ciphers supported by the remote server:
- High Strength Ciphers (>= 112-bit key)
* TLSv1 - n/a Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
* TLSv1 - n/a Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
* TLSv1 - AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
* TLSv1 - AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1

The fields above are:
* {OpenSSL ciphername}
* Kx={key exchange}
* Au={authentication}
* Enc={symmetric encryption method}
* Mac={message authentication code}
* {export flag}

Risk: Low

CVSS Score: *

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

OWASP: A2 - Broken Authentication and Session Management

More Information:
http://www.openssl.org/docs/apps/ciphers.html

TestID: 9819 (Revision: 2, Added: 2006-06-26)

3. HTTP PACKET INSPECTION / Web servers

Host(s) affected:
api.coralogix.com: https (443/tcp)

Summary:
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc.

api.coralogix.com : https (443/tcp)

```
Protocol version: HTTP/1.1
SSL: yes
Pipelining: yes
Keep-Alive: no
Options allowed: (Not implemented)
Headers:

Access-Control-Allow-Headers: undefined

Access-Control-Allow-Methods: undefined

Access-Control-Allow-Origin: *

Content-Type: text/plain, charset=utf-8

Date: Mon, 21 Jan 2019 08:35:19 GMT

ETag: W/"2-nOO9QiTIwXgNtWtBJezz8kv3SLc"

Vary: Accept-Encoding

X-Powered-By: Express

Content-Length: 2

Connection: keep-alive
```

Risk: Low

CVSS Score: *

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

TestID: 10209 (Revision: 1, Added: 2007-02-08)

Host Information

Information about host: api.coralogix.com

OS Detection:
api.coralogix.com

TestID: 2907

Nmap found that this host has an uptime of 32.653 days

TestID: 1043

Scanner IP: 10.0.0.149
Target IP: 34.252.191.230
Target Hostname: api.coralogix.com

TestID: 9162

unknown (443/tcp):

A SSL/TLS server answered on this port

TestID: 772

A web server is running on this port through SSL

TestID: 772

Information about host: coralogix-esapi.coralogix.com

Host Fully Qualified Domain Name:
coralogix-esapi.coralogix.com

TestID: 2907

Scanner IP: 10.0.0.149
Target IP: 34.247.139.218
Target Hostname: coralogix-esapi.coralogix.com

TestID: 9162

Web Scan Information

Authenticated Scan Configuration

Hostname: coralogix-esapi.coralogix.com
Web Site Authentication
Not configured. Click here to configure web site authentication.

URL and Content	Status	Failure Count	Test Count	Test Time

Authenticated Scan Configuration

Hostname: api.coralogix.com
Web Site Authentication
Not configured. Click here to configure web site authentication.

URL and Content	Status	Failure Count	Test Count	Test Time

What Next

Knowing is just half the battle. Now you have to go and fix the problems we reported above.

Intelligence gathering attacks may give attackers a good lead when trying to break into your host.

Denial-of-Service attacks are much more dangerous than they seem at first glance, for more information take a look at:

http://www.securiteam.com/securitynews/2JUQ6QAQTE.html

High risk vulnerabilities should be dealt with immediately. They give an attacker almost immediate access to your system! This is also a good time to review your logs and see if you could have identified this scan if it was performed without your knowledge. Conduct these penetration tests periodically to check for the newest attacks.