Vulnerability Report

Scan name:	Digicert_Scan
Host(s) scanned:	www.ispringsolutions.com
Date and time:	2020-05-10 05:27:37

Table of Contents

Report Summary

Scan name: Digicert_Scan

Host(s) scanned: www.ispringsolutions.com

Date and time: 2020-05-10 05:27:37

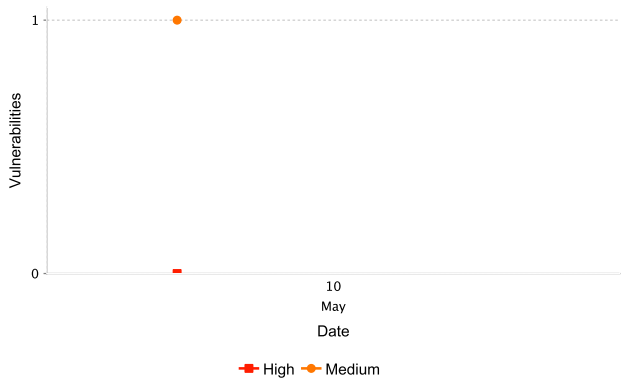
Time to finish: 15 minutes and 12 seconds to complete.

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.

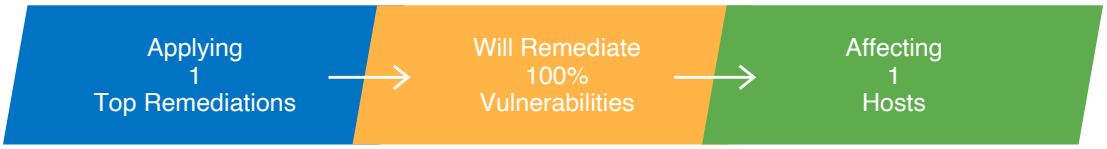
Vulnerability Trend

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



Remediation Focus

Repair the most common security issues on scan '**Digicert_Scan**' and 100% of its vulnerabilities will be resolved.



Top 1 remediations

1. Database Reachable from the Internet

Executive Summary

Overview					
Scan Name	Total	High	Medium	Low	Score *
Digicert_Scan	14	0	1	13	90.00

Vulnerabilities by Host and Risk Level					
Host	Total	High	Medium	Low	Score *
www.ispringsolutions.com Number of host(s): 1	14	0	1	13	90.00

Vulnerabilities by Service and Risk Level					
Service	Total	High	Medium	Low	Score *
general (icmp)	1	0	0	1	100.00
mpm-flags (44/tcp)	2	0	0	2	100.00
http (80/tcp)	1	0	0	1	100.00
ntp (123/udp)	1	0	0	1	100.00
https (443/tcp)	7	0	0	7	100.00
mysql (3306/tcp)	2	0	1	1	90.00

Vulnerabilities by Category					
Category	Total	High	Medium	Low	Score *
Web Applications	1	0	0	1	100.00
Web servers	6	0	0	6	100.00
Simple Network services	1	0	0	1	100.00
SSH servers	1	0	0	1	100.00
SQL servers	2	0	1	1	90.00
Encryption and Authentication	1	0	0	1	100.00
Preliminary Analysis	2	0	0	2	100.00

* The vulnerability score indicates the host's difficulty to hack on a scale from 0 to 100.

0 is very easy to gain unauthorized access, like easily exploited vulnerabilities or many potential unauthorized access points on the host.
100 is very difficult to gain unauthorized access, with no known vulnerabilities or only low risk vulnerabilities.

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.

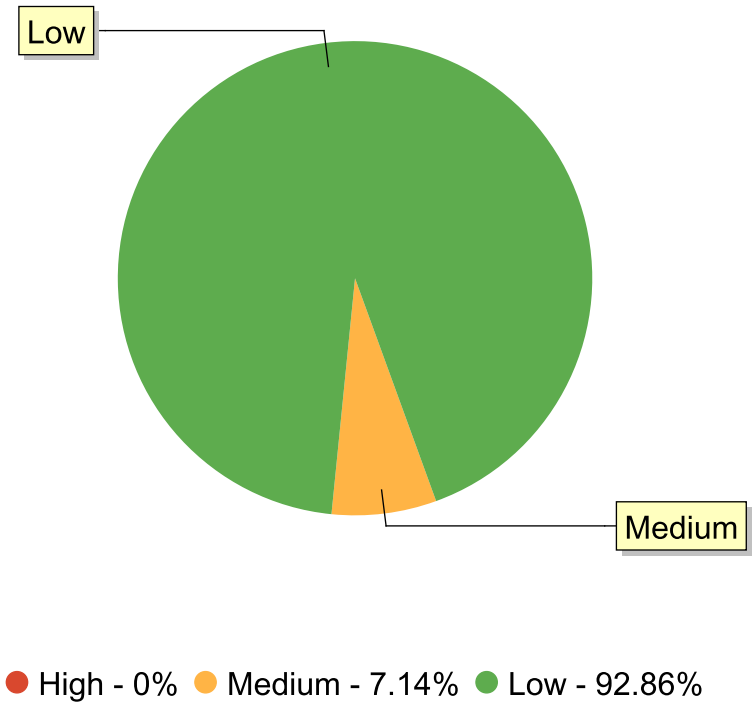
Other Issues

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.

Possible Vulnerabilities

Vulnerabilities Breakdown by Risk



1. DATABASE REACHABLE FROM THE INTERNET / SQL servers

Host(s) affected:
www.ispringsolutions.com: mysql (3306/tcp)

Summary
The remote host is running a database server that is reachable from the Internet.

www.ispringsolutions.com : mysql (3306/tcp)

A MySQL server is listening on this port.

Possible Solution
Filter incoming traffic to this port.

Risk: Medium

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: A9

More Information
http://en.wikipedia.org/wiki/PCI_DSS

TestID: 14263 (Revision: 1, Added: 2012-01-19)

1. DIRECTORY SCANNER / Web servers

Host(s) affected:
www.ispringsolutions.com: https (443/tcp)

Summary
We found some common directories on the web server:

www.ispringsolutions.com : https (443/tcp)

```
The following directories were discovered:
/docs, /help, /ispring/data, /ispring/logs, /bitrix, /blog/wp-content, /docs/display/~admin, /kb/docs/ultra
The following directories require authentication:
/webstats
```

Impact
This is usually not a security vulnerability, only an information gathering. Nevertheless, you should manually inspect these directories to ensure that they are in compliance with accepted security standards.

Possible Solution
Check if those directories contain any sensitive information, if they do, prevent unauthorized access to them.

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: 1822 (Revision: 5, Added: 2002-06-27)

2. 404 CHECK / Web Applications

Host(s) affected:
www.ispringsolutions.com: https (443/tcp)

Summary
This test tries to determine the best method to detect whether the remote server hosts a certain file.

The following string was used to determine that a file is not found on the server:
[]

www.ispringsolutions.com : https (443/tcp)

```
400 Bad Request
```

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: 1147 (Revision: 1, Added: 2000-01-01)

3. NTP VARIABLES READING / Simple Network services

Host(s) affected:
www.ispringsolutions.com: ntp (123/udp)

Summary
It is possible to determine a lot of information about the remote host by querying the NTP variables - these include OS descriptor, and time settings.

Theoretically one could work out the NTP peer relationships and track back network settings from this.

www.ispringsolutions.com : ntp (123/udp)

Impact
Attackers can gain critical information about the host.

Possible Solution
Set NTP to restrict default access to ignore all info packets: restrict default ignore

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: 1653 (Revision: 2, Added: 2000-01-01)

4. MYSQL SERVER VERSION DETECTION / SQL servers

Host(s) affected:
www.ispringsolutions.com: mysql (3306/tcp)

Summary
We detected a MySQL Server running on this port. The MySQL server version is:

www.ispringsolutions.com : mysql (3306/tcp)

Installed version: 5.7.27-30-log
Protocol: 10

Server Capabilities:
CLIENT_LONG_PASSWORD (new more secure passwords)
CLIENT_FOUND_ROWS (Found instead of affected rows)
CLIENT_LONG_FLAG (Get all column flags)
CLIENT_CONNECT_WITH_DB (One can specify db on connect)
CLIENT_NO_SCHEMA (Don't allow database.table.column)
CLIENT_COMPRESS (Can use compression protocol)
CLIENT_ODBC (ODBC client)
CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
CLIENT_IGNORE_SPACE (Ignore spaces before '(')
CLIENT_PROTOCOL_41 (New 4.1 protocol)
CLIENT_INTERACTIVE (This is an interactive client)
CLIENT_SSL (Switch to SSL after handshake)
CLIENT_SIGPIPE (IGNORE sigpipes)
CLIENT_TRANSACTIONS (Client knows about transactions)
CLIENT_RESERVED (Old flag for 4.1 protocol)
CLIENT_SECURE_CONNECTION (New 4.1 authentication)
Variant: Community Server

Possible Solution

To prevent attackers from gaining information on your MySQL server, change the version number to something generic (like: 0.0.0.0).

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: 1468 (Revision: 3, Added: 2000-01-01)

5. IDENTIFY UNKNOWN SERVICES VIA GET REQUESTS / Preliminary Analysis

Host(s) affected:

www.ispringsolutions.com: mpm-flags (44/tcp)

Summary

This test is a complement of Service test, as it tries recognize more banners and use an HTTP request if necessary.

www.ispringsolutions.com : mpm-flags (44/tcp)

A SSH server is running on this port

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: 8434 (Revision: 2, Added: 2005-04-06)

6. SSH SERVER BACKPORTED SECURITY PATCHES / SSH servers

Host(s) affected:

www.ispringsolutions.com: mpm-flags (44/tcp)

Summary

Security patches may have been 'back ported' to the remote SSH server without changing its version number. Banner-based checks have been disabled to avoid false positives.

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: 11776 (Revision: 1, Added: 2009-06-29)

7. NON-COMPLIANT STRICT TRANSPORT SECURITY (STS) / Web servers

Host(s) affected:

www.ispringsolutions.com: https (443/tcp)

Summary

The remote web server implements Strict Transport Security. However, it does not respect all the requirements of the STS draft standard.

www.ispringsolutions.com : https (443/tcp)

All connections to the HTTP site must be redirected to the HTTPS site.

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: 12059 (Revision: 1, Added: 2009-11-17)

8. STRICT TRANSPORT SECURITY (STS) DETECTION / Web servers

Host(s) affected:
www.ispringsolutions.com: https (443/tcp)

Summary
The remote web server implements Strict Transport Security (STS). The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

www.ispringsolutions.com : https (443/tcp)

```
The STS header line is:
Strict-Transport-Security: max-age=31536000
```

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: 12060 (Revision: 1, Added: 2009-11-17)

9. HTTP PACKET INSPECTION / Web servers

Host(s) affected:
www.ispringsolutions.com: http (80/tcp) 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.

www.ispringsolutions.com : http (80/tcp)

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

Date: Sun, 10 May 2020 05:20:09 GMT

Content-Type: text/html

Content-Length: 166

Connection: keep-alive

Location: https://www.ispringsolutions.com/

www.ispringsolutions.com : https (443/tcp)

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

Date: Sun, 10 May 2020 05:20:08 GMT

Content-Type: text/html, charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=sq9mdbpd2asf47er2br6947n6s, path=/, HTTPOnly, Secure

Expires: Sun, 10 May 2020 06:20:08 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: public

P3P: policyref="/bitrix/p3p.xml", CP="NON DSP COR CUR ADM DEV PSA PSD OUR UNR ... X-Powered-CMS: Bitrix Site Manager (47ccdc19172104a75ebd41461fde81a0)

Set-Cookie: isgaexp_7k-e9uvwRIGLn-inLdD2OA=1, expires=Sun, 07-Jun-2020 05:20:0... Vary: Accept-Encoding

Strict-Transport-Security: max-age=31536000,

Content-Security-Policy-Report-Only: default-src https: wss: data: blob:, scri...

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)

10. SITEMAP.XML FILE AND DIRECTORY ENUMERATION / Web servers

Host(s) affected:

www.ispringsolutions.com: https (443/tcp)

Summary

The Sitemap file informs search engines about the available pages on your websites. In its simplest form, a Sitemap is an XML file that lists URLs for a site.

This is usually not a security vulnerability, but it does help a potential attacker when gathering intelligence. You should go over the list below and make sure all the pages listed are 'public' pages that are not supposed to be hidden or confidential.

www.ispringsolutions.com : https (443/tcp)

/sitemap.xml
<loc>https://www.ispringsolutions.com/sitemap_so...</loc>
<loc>https://www.ispringsolutions.com/sitemap_do...</loc>
<loc>https://www.ispringsolutions.com/sitemap_ar...</loc>
<loc>https://www.ispringsolutions.com/blog/sitem...</loc>
<loc>https://www.ispringsolutions.com/blog/sitem...</loc>

Impact

None, only an intelligence gathering method

Possible Solution
Site owners should review the contents of there sitemap.xml file for sensitive material.

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: A5

More Information
https://www.google.com/sitemaps/protocol.html

TestID: 10025 (Revision: 3, Added: 2006-10-15)

11. ICMP TIMESTAMP REQUEST / Preliminary Analysis

Host(s) affected:
www.ispringsolutions.com: general (icmp)

Summary
The remote host answers to an ICMP timestamp request. This allows an attacker to know the time and date on your host.

Impact
This may help attackers to defeat time based authentications schemes.

Possible Solution
See solution provided at: https://beyondsecurity.zendesk.com/hc/en-us/articles/203609549--How-can-I-mitigate-ICMP-Timestamp-

Risk: Low

CVSS Score: 0.00

OWASP: A6

CVSS Score: 0.00

CVSS: AV:L/AC:L/Au:N/C:N/I:N/A:N

CVE: CVE-1999-0524

Microsoft Knowledge Base: 313190

More Information
http://www.beyondsecurity.com/faq/questions/54/how-can-i-mitigate-icmp-timestamp, https://beyondsecurity.zendesk.com/hc/en-us/articles/203609549--How-can-I-mitigate-ICMP-Timestamp-, https://social.technet.microsoft.com/Forums/

windows/en-US/219f3dcc-3e5b-4d9b-88ae-137215575c7f/icmp-timestamp-response?forum=w7itprosecurity

TestID: 811 (Revision: 6, Added: 2000-01-01)

12. SSL VERIFICATION TEST / Encryption and Authentication

Host(s) affected:
www.ispringsolutions.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.

www.ispringsolutions.com : https (443/tcp)

Here is the server certificate:
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
05:98:3e:28:41:ec:21:05:83:d2:2a:65:83:b9:f5:03
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, CN=DigiCert Global CA G2
Validity
Not Before: Nov 30 00:00:00 2018 GMT
Not After : Dec 13 12:00:00 2020 GMT
Subject: businessCategory=Private Organization/1.3.6.1.4.1.311.60.2.1.3=US/1.3.6.1.4.1.311.60.2.1.2=Virginia/serialNumber=06876585, C=US, ST=Virginia, L=Alexandria, O=iSpring Solutions, Inc., CN=www.ispringsolutions.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:ba:63:d4:92:ee:61:02:82:01:b8:29:ce:b7:6b:
8e:95:bf:aa:09:73:f1:87:ca:67:6c:c4:b0:7d:7b:
e1:b3:bc:89:ee:d5:0f:22:44:af:bb:c1:84:84:5d:
c9:ae:7c:2e:5f:06:42:7e:29:62:4f:0d:62:0f:7f:
8d:1f:04:e7:8c:c7:31:1a:3a:f6:e6:10:d9:4a:94:
9c:74:13:e0:e2:cf:f4:0d:18:85:4e:77:bd:ac:d9:
2d:18:8c:8d:00:8b:02:1f:e4:c8:33:3d:53:18:56:
32:c0:dc:66:7c:d7:bd:49:52:36:38:29:80:61:11:
ae:9f:25:86:e9:9d:72:c3:ed:cf:a1:1e:83:78:91:
1a:98:4a:b2:5e:3b:4a:2f:23:72:91:f8:c7:6f:2f:
a7:a9:b5:50:09:b7:b8:e6:f0:1a:03:b8:94:9a:9a:

98:bc:32:00:19:fd:e5:5e:b8:e5:3a:f1:26:29:d7:
95:53:05:8a:4f:82:88:40:fc:f9:78:68:65:31:dd:
87:12:70:8a:8a:a6:3e:06:44:e2:e3:e2:48:84:56:
bc:85:83:ec:d1:8a:f8:ac:50:62:dc:2e:ac:6a:4e:
81:66:90:8a:52:2c:18:4e:cd:75:70:32:3f:db:59:
d7:df:e5:53:0a:9c:10:88:c8:d2:21:00:77:fe:47:
d6:99
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:24:6E:2B:2D:D0:6A:92:51:51:25:69:01:AA:9A:47:A6:89:E7:40:20

X509v3 Subject Key Identifier:
32:1E:A5:E7:6C:F2:61:1A:03:0D:E8:42:49:56:46:54:44:D7:EC:2A
X509v3 Subject Alternative Name:
DNS:www.ispringsolutions.com, DNS:ispringsolutions.com
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 CRL Distribution Points:

Full Name:
URI:http://crl3.digicert.com/DigiCertGlobalCAG2.crl

Full Name:
URI:http://crl4.digicert.com/DigiCertGlobalCAG2.crl

X509v3 Certificate Policies:
Policy: 2.16.840.1.114412.2.1
CPS: https://www.digicert.com/CPS
Policy: 2.23.140.1.1

Authority Information Access:
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/DigiCertGlobalCAG2.crt

X509v3 Basic Constraints:
CA:FALSE
1.3.6.1.4.1.11129.2.4.2:
...m.k.w.....q...#...{G8W.
.R....d6.....ge

#C.....H0F.!..`..=(.....jQ.&..S.+.U.....'@...!.....%&..0.4.....y.L.....{.PP.w.V.../.....D.>.Fv....\....U.....ge
#.....H0F.!....N!%A`.z.s-.....:..
pdBEt7N@'.!....Y.....LQ.Q6:h....:..t..D.Q..w..u..Y|..C._..n.V.GV6.J.`....^.....ge
%.....H0F.!..hp...[..&.R..u*.(....n...:J.....!..i1.....? ...g..A...I&sM.v=.1.X.
Signature Algorithm: sha256WithRSAEncryption
a6:a9:f6:e4:84:e4:9b:a2:5a:6e:81:af:30:73:87:d8:94:28:
4a:7f:5f:12:89:20:3a:ee:35:22:0c:af:61:e0:9f:a6:3c:46:
82:e0:33:92:ec:e9:4f:d8:ea:68:09:ff:20:56:8c:54:19:15:
94:38:86:5e:70:66:73:73:4d:fe:3d:93:57:33:45:1a:cb:0a:
68:d8:bf:e3:c6:a5:f2:5d:53:58:ac:cd:9a:44:bc:e6:fd:37:
1a:e6:a9:87:31:17:30:d7:f7:0f:fb:cb:2b:a3:af:65:7f:0e:
2b:05:55:23:c9:fe:36:9e:b4:e2:2c:fb:13:25:c2:30:9d:72:
d1:7c:b4:7c:cd:62:76:da:f8:5b:0e:5b:33:49:25:22:af:6f:
5b:d1:3a:e4:2a:48:cd:df:a4:72:e7:88:c8:a3:f0:97:a3:28:
a4:30:8d:04:7e:64:33:65:8e:da:b4:d4:30:39:33:ab:c2:13:
75:5b:cb:e8:b5:28:62:81:95:6f:d6:8b:42:5a:6b:68:3d:08:
27:9e:3d:b1:c2:e6:6c:c3:fb:97:32:04:43:2e:e9:48:67:b7:
a0:31:47:e3:12:3c:73:96:54:3d:45:ac:44:41:62:78:e8:65:
01:83:59:24:de:a2:ac:8c:15:12:db:fe:55:d1:a3:85:b4:09:
84:76:a8:0e
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)

Host Information

Information about host: www.ispringsolutions.com

Host Fully Qualified Domain Name:
Scanner IP: 10.0.201.248
Target IP: 69.167.164.201
Target Hostname: www.ispringsolutions.com

TestID: 9162
www.ispringsolutions.com

TestID: 2907

general (icmp): Port found open

mpm-flags (44/tcp):
An ssh server is running on this port

TestID: 772

SSH version: SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u4

TestID: 942
The remote SSH daemon supports the following versions of the SSH protocol:

. 1.99
. 2.0

TestID: 1642

http (80/tcp):
A web server is running on this port

TestID: 772

https (443/tcp):
A SSL/TLS server answered on this port

TestID: 772
A web server is running on this port through SSL

TestID: 772