脆弱性アセスメントレポート

診断名:	Digicert_Scan
ホスト名/IPアドレス:	[redacted]
スキャン日時:	2018-08-26 08:02:13

目次

レポート概要

診断名: Digicert_Scan

ホスト名/IPアドレス: [redacted]

スキャン日時: 2018-08-26 08:02:13

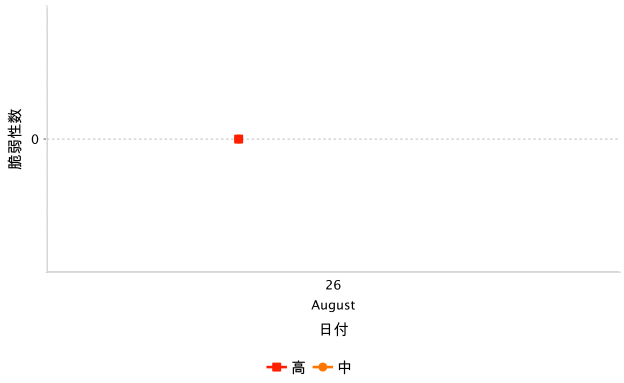
所要時間: 12 分 12 秒

レポートの「脆弱性/脆弱性の疑い」項目では、診断中に検知された脆弱性を危険度別に表示しています。なお　診断では、実際にこの脆弱性を利用した攻撃を実施したわけではございません、このためレポートには脆弱性の疑いがあると判定された結果が含まれております。

検知内容には直ちに対策を要す脆弱性ではありませんが、注意の必要な脆弱性を含みます；攻撃者が不正にアクセス権を取得するために直接的に役立つ情報ではありませんが、ローカルネットワークやホスト情報を与えることができる場合、このような結果は「危険度低/機密情報収集」と分類されます。

脆弱性の傾向

スキャン(診断名: Digicert_Scan)で検知された危険度高と中の合計数の変化



解決策

診断結果からより一般的なセキュリティの問題を修正します (診断名: Digicert_Scan)。それらを修正することにより0%の脆弱性が解決できます。

Top 0 remediations

エグゼクティブサマリー

概要					
スキャン名	合計	高	中	低	スコア *
Digicert_Scan	10	0	0	10	100.00

ホスト別、危険度別の脆弱性					
ホスト	合計	高	中	低	スコア *
[redacted]	10	0	0	10	100.00
ホスト数 1					

サービス別、危険度別の脆弱性					
サービス	合計	高	中	低	スコア *
general (tcp)	1	0	0	1	100.00
ssh (22/tcp)	1	0	0	1	100.00
http (80/tcp)	3	0	0	3	100.00
https (443/tcp)	5	0	0	5	100.00

カテゴリ別の脆弱性					
カテゴリ	合計	高	中	低	スコア *
ウェブサーバ	4	0	0	4	100.00
情報収集	4	0	0	4	100.00
暗号化と認証	2	0	0	2	100.00

脆弱性のスコアは、ホストに対するハッキングの実現可能性を0から100までの目盛りで示しています。0は、容易に脆弱性を利用することができる状態にある、またはホスト上に多くの潜在的な不正アクセスポイントがあるなど、簡単に不正なアクセスができる状態にあります。
100は、既知の脆弱性がない、または非常に低リスクな脆弱性のみが存在している状態で、不正なアクセスをし難いという状況を現しています。

エグゼクティブサマリー

レポート内の脆弱性は、高・中・低の3つのカテゴリに分類されます。この分類は業界標準に基づいており、主要なクレジットカード会社が承認する標準に基づいています。以下がカテゴリの定義です：

危険度高の脆弱性

次のカテゴリーに該当するものが振り分けられています：バックドア、ファイルに対する読み込み・書き込み権限、リモートでのコマンドの実行、トロイの木馬、パスワードなどの機密情報漏洩

危険度中の脆弱性

危険度高には分類されないが、次の項目に該当するものが振り分けられています：ホストのファイルに対する限定的なアクセス、ディレクトリー・トラバーサル、セキュリティの仕組みの漏えい（フィルターのルールなど）、DoS攻撃、メールリレーなどの不正なサービス利用

危険度低の脆弱性

危険度高・中に分類されないものが振り分けられています。具体的には、次の項目が含まれます：サーバ構成についての機密情報など、情報収集の検査

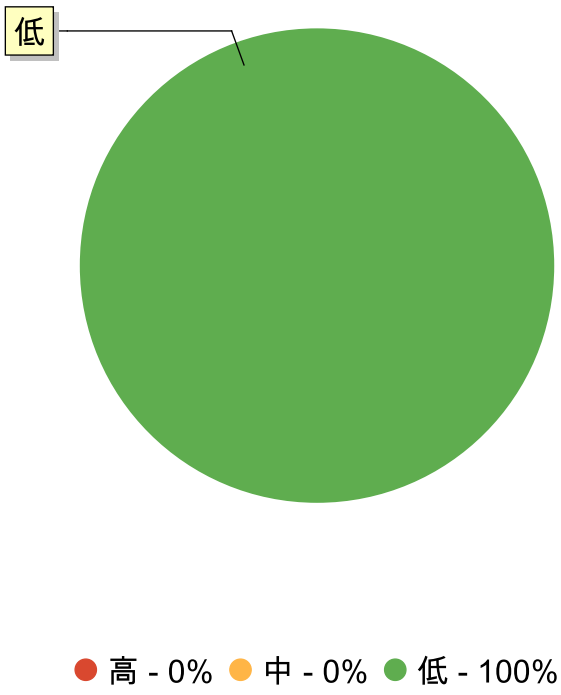
その他の問題

ホスト情報 - 対象ホストについて各テストで検知した情報や、脆弱性として分類されない検査結果です。

推測されたプラットフォーム - このホスト上で稼動しているOSの検知で、TCP/IPスタックのフィンガープリントを使っているので、不正確な場合があり、推測となります。

可能性のある脆弱性

危険度別の脆弱性内訳



1. DIRECTORY SCANNER / ウェブサーバ

影響のあるホスト

[redacted]: http (80/tcp) https (443/tcp)

概要

We found some common directories on the web server:

[redacted] : http (80/tcp)

The following directories were discovered:
/admin, /icons

[redacted] : https (443/tcp)

The following directories were discovered:
/icons

影響

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.

一般的な解決方法

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

リスク: 低

CVSS値: *

注意: この脆弱性は、NIST National Vulnerability Database には含まれていません。PCI DSS には、CVSSスコアリングシステムを使用して、危険度スコアが必要となります

検査ID: 1822 (修正: 5, 追加: 2002-06-27)

2. SSL VERIFICATION TEST / 暗号化と認証

影響のあるホスト

[redacted]: https (443/tcp)

概要

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

[redacted] : https (443/tcp)

Here is the server certificate:
Certificate:
Data:
Version: 3 (0x2)
Serial Number:

04:fc:d7:f2:07:c3:79:1d:e9:f4:e0:5d:85:b4:4f:8a
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, CN=[redacted]
Validity
Not Before: Jun 26 00:00:00 2018 GMT
Not After : Jun 26 12:00:00 2019 GMT
Subject: C=JP, ST=TOKYO, L=CHUO-KU, O=DigiCert JAPAN G.K., OU=internal, CN=[redacted]
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:83:56:4d:f8:53:d2:8f:e4:e2:de:2b:a7:ce:df:
1d:78:22:29:dd:0a:79:dc:87:8d:74:59:f3:c7:85:
11:0e:39:27:e9:cd:66:1d:38:28:9e:7e:0e:d0:b0:
25:a9:d3:b6:bd:89:92:34:c1:2b:79:61:b2:3a:ad:
36:e9:2a:ba:36:03:b9:54:13:b2:e7:f3:67:45:62:
26:2b:17:55:db:6d:3e:2f:b2:8b:76:95:ed:26:70:
4a:18:12:59:36:53:cd:cc:3d:21:55:4b:45:35:60:
5f:e9:5d:a8:bf:ac:71:44:2b:95:5a:9b:ad:47:ca:
a8:02:ff:b5:8a:47:c0:ec:7d:22:85:9b:8b:be:e5:
e1:a5:5a:0f:ea:67:68:45:8d:0d:91:48:cd:fc:6e:
61:4e:bd:19:c1:57:73:af:3a:d4:35:ef:f2:9a:d4:
39:4c:bc:6e:e5:11:e2:36:1f:f0:b3:24:9a:ee:b6:
06:29:6f:f5:ed:2f:9a:17:7b:e7:dd:86:f7:14:6b:
c9:8f:b1:8e:da:e7:02:38:3b:c1:fa:28:43:df:4f:
ec:98:b8:13:41:45:53:fd:a5:98:ac:a0:a8:8f:0c:
a9:a6:4a:f8:be:e7:a1:a3:eb:3c:79:2a:b9:0a:49:
a4:64:a9:92:2d:75:ad:1e:04:d3:ad:35:1b:52:56:
d5:19
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:0F:80:61:1C:82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2

X509v3 Subject Key Identifier:
DA:A9:4B:FD:98:AA:95:FD:19:77:7B:92:19:AE:FA:8F:35:F1:F5:8C
X509v3 Subject Alternative Name:
DNS:[redacted]
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/ssca-sha2-g6.crl

Full Name:
URI:http://crl4.digicert.com/ssca-sha2-g6.crl

X509v3 Certificate Policies:
Policy: 2.16.840.1.114412.1.1
CPS: https://www.digicert.com/CPS
Policy: 2.23.140.1.2.2

Authority Information Access:
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt

X509v3 Basic Constraints:
CA:FALSE
1.3.6.1.4.1.11129.2.4.2:
.....u.....X.....gp
<5.....w...
.....d=0
.....F0D. Ft.
0..6..t..x.+.#.}....0_z.B.Y1. @.e...1j..<.....}.....n|...Wy<..u..u..Y|..C._..n.V.GV6.J.`....^.....d=0.....F0D.
8X...k.....'.....s.....X. ...c..c....6A.Y..F\.|...D}..:.9.
Signature Algorithm: sha256WithRSAEncryption
86:41:fb:9c:5c:b0:ea:5c:49:c7:b0:32:42:23:1b:81:54:35:
a4:2d:e6:4c:8d:80:b9:eb:be:05:9c:78:ab:10:f0:32:57:3b:
63:b7:e5:fd:11:2a:82:6f:6e:aa:31:a1:af:20:0b:8c:3f:20:
87:f1:1a:90:7f:3c:3f:e9:56:3b:41:9a:06:b1:50:2c:77:57:
db:24:14:b4:d3:87:2b:78:62:92:d4:c9:3c:b9:3a:0b:ab:04:
aa:e0:63:dd:2c:aa:bd:10:a5:5e:27:be:55:0f:a6:98:b8:0b:
9c:a8:af:ad:8e:d8:d7:eb:24:76:05:a2:4e:a8:0d:5b:81:bd:
33:aa:12:ba:58:a2:5a:91:58:86:09:3b:57:55:5b:bd:84:f1:
0f:85:c8:68:d6:fe:0e:ba:77:b9:35:f2:be:5c:61:e8:25:e5:
17:42:c3:b2:24:71:6c:69:8c:2f:e8:68:01:fd:a2:17:f2:53:
d4:28:ad:08:e2:fb:d5:7b:66:a3:10:d6:35:16:60:b4:4b:1c:
4f:c9:ea:50:2c:b9:63:8e:ae:18:11:0a:fd:3b:72:1b:07:58:
ad:c0:e7:c2:7f:3a:b9:89:3f:01:a6:a1:5f:71:14:97:82:cf:
4b:24:2d:21:01:d1:b9:14:6d:e2:c2:79:d5:9c:80:21:dd:65:
90:f9:c1:1e
This SSLv2 server does not accept SSLv3 connections.
This SSLv2 server also accepts TLSv1 connections.

一般的な解決方法
Usage of weak ciphers should be avoided.

リスク: 低

CVSS値: *
注意: この脆弱性は、NIST National Vulnerability Database には含まれていません。PCI DSS には、CVSSスコアリングシステムを使用して、危険度スコアが必要となります
検査ID: 2804 (修正: 4, 追加: 2003-12-25)

3. IDENTIFY UNKNOWN SERVICES VIA GET REQUESTS / 情報収集

影響のあるホスト
[redacted]: http (80/tcp) https (443/tcp) ssh (22/tcp)

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

[redacted] : http (80/tcp)

A web server is running on this port

[redacted] : https (443/tcp)

A web server is running on this port

[redacted] : ssh (22/tcp)

A SSH server is running on this port

リスク: 低

CVSS値: *
注意: この脆弱性は、NIST National Vulnerability Database には含まれていません。PCI DSS には、CVSSスコアリングシステムを使用して、危険度スコアが必要となります
検査ID: 8434 (修正: 2, 追加: 2005-04-06)

4. SUPPORTED SSL CIPHERS SUITES / 暗号化と認証

影響のあるホスト
[redacted]: https (443/tcp)

概要

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

[redacted] : 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
* TLSv1 - n/a Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
* TLSv1 - n/a Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1

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

リスク: 低

CVSS値: *

注意: この脆弱性は、NIST National Vulnerability Database には含まれていません。PCI DSS には、CVSSスコアリングシステムを使用して、危険度スコアが必要となります

OWASP: A2

追加情報

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

検査ID: 9819 (修正: 2, 追加: 2006-06-26)

5. HTTP PACKET INSPECTION / ウェブサーバ

影響のあるホスト

[redacted]: http (80/tcp) https (443/tcp)

概要

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

[redacted] : http (80/tcp)

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

Server: nginx/1.12.1

Date: Sun, 26 Aug 2018 07:57:49 GMT

Content-Type: text/html

Content-Length: 3839

Last-Modified: Thu, 14 Jun 2018 04:51:36 GMT

Connection: keep-alive

ETag: "5b21f458-eff"

Accept-Ranges: bytes

[redacted] : https (443/tcp)

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

Server: nginx/1.12.1

Date: Sun, 26 Aug 2018 07:57:49 GMT

Content-Type: text/html

```
Content-Length: 1302

Last-Modified: Mon, 02 Jul 2018 02:10:25 GMT

Connection: keep-alive

ETag: "5b398991-516"

Accept-Ranges: bytes
```

リスク: 低

CVSS値: *

注意: この脆弱性は、NIST National Vulnerability Database には含まれていません。PCI DSS には、CVSSスコアリングシステムを使用して、危険度スコアが必要となります

検査ID: 10209 (修正: 1, 追加: 2007-02-08)

6. TCP TIMESTAMPS RETRIEVAL / 情報収集

影響のあるホスト

[redacted]: general (tcp)

概要

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can be sometimes be computed.

[redacted] : general (tcp)

```
The uptime was estimated to 370290s, i.e. about 4 days.
(Note that the clock is running at about 1050 Hz and will overflow in about 4090444s, that is 47 days)
```

リスク: 低

CVSS値: *

注意: この脆弱性は、NIST National Vulnerability Database には含まれていません。PCI DSS には、CVSSスコアリングシステムを使用して、危険度スコアが必要となります

OWASP: A6

追加情報

http://www.ietf.org/rfc/rfc1323.txt

検査ID: 10399 (修正: 1, 追加: 2007-05-27)

ホスト情報

ホストに関する情報: [redacted]

OS Detection:
[redacted]

検査ID: 2907
Nmap found that this host has an uptime of 4.495 days

検査ID: 1043
Scanner IP: [redacted]
Target IP: [redacted]
Target Hostname: [redacted]

検査ID: 9162

ssh (22/tcp):
An ssh server is running on this port

検査ID: 772

SSH version: SSH-2.0-OpenSSH_7.4
SSH supported authentication: publickey

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

. 1.99
. 2.0

SSHv2 host key fingerprint : c4:10:3f:12:2d:27:67:7c:9d:b1:44:ca:e1:39:4a:66

検査ID: 1642

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

検査ID: 772
nginx/1.12.1

検査ID: 1035

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

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

検査ID: 772
nginx/1.12.1

検査ID: 1035