ASV Scan Report
Vulnerability Details

UserVoice Inc.
Scan Results

## Executive Summary

<table>
<thead>
<tr>
<th>PCI Compliance: Passing</th>
<th>Scan Target: app.uservoice.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan ID: 6219680</td>
<td>Start: 2015-06-15 21:00:01</td>
</tr>
<tr>
<td>Maximum score: 3.9</td>
<td>Finish: 2015-06-16 17:25:48</td>
</tr>
<tr>
<td>Scan Length: 20:25:47</td>
<td>Scan Expiration: 2015-09-19</td>
</tr>
<tr>
<td>TCP/IP Fingerprint OS Estimate: Crestron XPanel control system</td>
<td></td>
</tr>
</tbody>
</table>

SecurityMetrics has determined that UserVoice Inc. is COMPLIANT with the PCI scan validation requirement for this computer. Congratulations, the computer passes because no failing vulnerability was found.

If SecurityMetrics scanned your website, you may choose to use our certified logo. This logo cannot be used if we have only scanned your network, and is only valid for use on websites scanned and passing by SecurityMetrics. Your Site Certification ID is: 735742. Please keep this number. How To Add Certified Logo.

Attackers typically use footprinting, port scanning and security vulnerability scanning to find security weaknesses on computers. This report provides information on each of these categories.

### Footprinting

Footprinting is finding public information regarding this IP which an attacker could use to gain access.

### Port Scan

Attackers use a port scan to find out what programs are running on your computer. Most programs have known security weaknesses. Disable any unnecessary programs listed below.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Program</th>
<th>Status</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>Ping</td>
<td></td>
<td>Accepting</td>
<td>Your computer is answering ping requests.</td>
</tr>
<tr>
<td>TCP</td>
<td>80</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>Your computer appears to be running http software that allows others to view its web pages. If you don't intend this computer to allow others to view its web pages then turn this service off. There are many potential security vulnerabilities in http software.</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>Your computer appears to be running HTTP Secure Socket Layer (SSL) software. This software improves the security of HTTP communication with this server.</td>
</tr>
<tr>
<td>TCP</td>
<td>2052</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>2053</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.</td>
</tr>
</tbody>
</table>
## Security Vulnerabilities Solution Plan

The following section lists all security vulnerabilities detected on your system. Vulnerabilities which cause you to fail PCI compliance have a score listed in red.

### PCI Risk Table

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Program</th>
<th>Score</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>2082</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>2083</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>2086</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>2087</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>2095</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>2096</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>8080</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>8443</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>A program is listening on this port. This helps a hacker to gather information about what is running on this machine and what kind of machine you have. If you do not require this program to be listening on this port, turn it off.</td>
</tr>
<tr>
<td>TCP</td>
<td>8880</td>
<td>cloudflare-nginx</td>
<td>Open</td>
<td>Your computer is responding to scans on this port. This helps a hacker to gather information about possible services running on this machine and what kind of machine you have. If you do not require this service turn it off.</td>
</tr>
</tbody>
</table>
### Description:
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability

### Synopsis:
It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

### Impact:
A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This script tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite, and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the `SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS` option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord`.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not, depending on whether or not a countermeasure has been enabled. Note that this script detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

See also: [http://www.openssl.org/~bodo/tls-cbc.txt](http://www.openssl.org/~bodo/tls-cbc.txt)  
[http://support.microsoft.com/kb/2643584](http://support.microsoft.com/kb/2643584)  

### Data Received:
Negotiated cipher suite: AES128-SHA|TLSv1|Kx=RSA|Au=RSA|Enc=AES- CBC(128)|Mac=SHA1

### Resolution:
Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

### Risk Factor:
Low/ CVSS2 Base Score: 3.9

(AV:N/AC:M/Au:N/C:P/I:N/A:N) **CVE:** [CVE-2011-3389](http://www.cvedetails.com/cve/CVE-2011-3389)
Description: SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability

Synopsis: It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Impact: A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This script tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite, and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the "SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS" option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key H KEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not, depending on whether or not a countermeasure has been enabled. Note that this script detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.


Data Received: Negotiated cipher suite: AES128-SHA|TLSv1|Kx=RSA|Au=RSA|Enc=AES- CBC(128)|Mac=SHA1

Resolution: Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Risk Factor: Low/ CVSS2 Base Score: 3.9 (AV:N/AC:M/Au:N/C:P/I:N/A:N) CVE: CVE-2011-3389
<table>
<thead>
<tr>
<th>TCP</th>
<th>8443</th>
<th>psecync-https</th>
<th><strong>2.6</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>Transport Layer Security (TLS) Protocol CRIME Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Synopsis:</strong></td>
<td>The remote service has a configuration that may make it vulnerable to the CRIME attack.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Impact:</strong></td>
<td>The remote service has one of two configurations that are known to be required for the CRIME attack:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>SSL / TLS compression is enabled. - TLS advertises the SPDY protocol earlier than version 4.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note that SecurityMetrics did not attempt to launch the CRIME attack against the remote service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>See also:</td>
<td><a href="http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091">http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Received:</strong></td>
<td>The following configuration indicates that the remote service may be vulnerable to the CRIME attack:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>SPDY support earlier than version 4 is advertised.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resolution:</strong></td>
<td>Disable compression and / or the SPDY service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Factor:</strong></td>
<td>Low/ CVSS2 Base Score: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) CVE: CVE-2012-4930 Additional CVEs: CVE-2012-4929</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP</th>
<th>443</th>
<th>https</th>
<th><strong>2.6</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>Transport Layer Security (TLS) Protocol CRIME Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Synopsis:</strong></td>
<td>The remote service has a configuration that may make it vulnerable to the CRIME attack.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Impact:</strong></td>
<td>The remote service has one of two configurations that are known to be required for the CRIME attack:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>SSL / TLS compression is enabled. - TLS advertises the SPDY protocol earlier than version 4.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note that SecurityMetrics did not attempt to launch the CRIME attack against the remote service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>See also:</td>
<td><a href="http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091">http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Received:</strong></td>
<td>The following configuration indicates that the remote service may be vulnerable to the CRIME attack:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>SPDY support earlier than version 4 is advertised.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resolution:</strong></td>
<td>Disable compression and / or the SPDY service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Factor:</strong></td>
<td>Low/ CVSS2 Base Score: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) CVE: CVE-2012-4930 Additional CVEs: CVE-2012-4929</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Description:** SSL Cipher Suites Supported

**Synopsis:** The remote service encrypts communications using SSL.

**Impact:** This script detects which SSL ciphers are supported by the remote service for encrypting communications.

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

**Data Received:** Here is the list of SSL ciphers supported by the remote server:

Each group is reported per SSL Version.

**SSL Version: TLSv12**

High Strength Ciphers (>= 112-bit key)

- ECDHE-RSA-DES-CBC3-SHA
  Kx=ECDH Au=RSA Enc=3DES-CBC(168)
  Mac=SHA1
- ECDHE-RSA-AES128-SHA
  Kx=ECDH Au=RSA Enc=AES-CBC(128)
  Mac=SHA1
- ECDHE-RSA-AES256-SHA
  Kx=ECDH Au=RSA Enc=AES-CBC(256)
  Mac=SHA1
- ECDHE-RSA-AES128-SHA256
  Kx=ECDH Au=RSA Enc=AES-CBC(128)
  Mac=SHA256
- ECDHE-RSA-AES256-SHA384
  Kx=ECDH Au=RSA Enc=AES-CBC(256)
  Mac=SHA384

**SSL Version: TLSv11**

High Strength Ciphers (>= 112-bit key)

- ECDHE-RSA-DES-CBC3-SHA
  Kx=ECDH Au=RSA Enc=3DES-CBC(168)
  Mac=SHA1
- ECDHE-RSA-AES128-SHA
  Kx=ECDH Au=RSA Enc=AES-CBC(128)
  Mac=SHA1
- ECDHE-RSA-AES256-SHA
  Kx=ECDH Au=RSA Enc=AES-CBC(256)
  Mac=SHA1
- ECDHE-RSA-AES128-SHA256
  Kx=ECDH Au=RSA Enc=AES-CBC(128)
  Mac=SHA256
- ECDHE-RSA-AES256-SHA384
  Kx=ECDH Au=RSA Enc=AES-CBC(256)
  Mac=SHA384

**SSL Version: TLSv1**

High Strength Ciphers (>= 112-bit key)

- ECDHE-RSA-DES-CBC3-SHA
  Kx=ECDH Au=RSA Enc=3DES-CBC(168)
  Mac=SHA1
- ECDHE-RSA-AES128-SHA
  Kx=ECDH Au=RSA Enc=AES-CBC(128)
  Mac=SHA1
- ECDHE-RSA-AES256-SHA
  Kx=ECDH Au=RSA Enc=AES-CBC(256)
  Mac=SHA1
- ECDHE-RSA-AES128-SHA256
  Kx=ECDH Au=RSA Enc=AES-CBC(128)
  Mac=SHA256
- ECDHE-RSA-AES256-SHA384
  Kx=ECDH Au=RSA Enc=AES-CBC(256)
  Mac=SHA384

The fields above are:


**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
### Description: SSL Cipher Block Chaining Cipher Suites Supported

**Synopsis:** The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

**Impact:** The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

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

**Data Received:** Here is the list of SSL CBC ciphers supported by the remote server: High Strength Ciphers (>= 112-bit key)

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Key Exchange</th>
<th>Authentication</th>
<th>Symmetric Encryption Method</th>
<th>Message Authentication Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1 ECDHE-RSA-DES-CBC3-SHA Kx=ECDH Au=RSA Enc=3DES-CBC(168) Mac=SHA1 ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1 ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1 DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1 AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1 AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1 ECDHE-RSA-AES128-SHA256 Kx=ECDHE Au=RSA Enc=AES-CBC(128) Mac=SHA256 ECDHE-RSA-AES256-SHA384 Kx=ECDHE Au=RSA Enc=AES-CBC(256) Mac=SHA384 RSA-AES128-SHA256 Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA256 RSA-AES256-SHA256 Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA256</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The fields above are:

{OpenSSL ciphername} Kx={key exchange} Au={authentication} Enc={symmetric encryption method} Mac={message authentication code} {export flag}

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

### Description: OpenSSL Detection

**Synopsis:** The remote service appears to use OpenSSL to encrypt traffic.

**Impact:** Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See also:

http://www.openssl.org

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Service</th>
<th>Risk Factor</th>
<th>CVSS Base Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>2096</td>
<td>nbx-dir</td>
<td>Low</td>
<td>1.0</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>https</td>
<td>Low</td>
<td>1.0</td>
</tr>
<tr>
<td>TCP</td>
<td>8443</td>
<td>pcsync-https</td>
<td>Low</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Description:** HTTP Server Type and Version

**Synopsis:** A web server is running on the remote host.

**Impact:** This plugin attempts to determine the type and the version of the remote web server.

**Data Received:** The remote web server type is: cloudflare-nginx

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Version</th>
<th>Description:</th>
<th>Synopsis:</th>
<th>Impact:</th>
<th>Data Received:</th>
<th>Resolution:</th>
<th>Risk Factor:</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>https</td>
<td>OpenSSL Detection</td>
<td>The remote service appears to use OpenSSL to encrypt traffic.</td>
<td>Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.</td>
<td>Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).</td>
<td>n/a</td>
<td>Low/ CVSS2 Base Score: 1.0</td>
</tr>
<tr>
<td>8880</td>
<td>TCP</td>
<td>cddbp-alt</td>
<td>HTTP Server Type and Version</td>
<td>A web server is running on the remote host.</td>
<td>This plugin attempts to determine the type and the version of the remote web server.</td>
<td>The remote web server type is: cloudflare-nginx</td>
<td>n/a</td>
<td>Low/ CVSS2 Base Score: 1.0</td>
</tr>
<tr>
<td>2087</td>
<td>TCP</td>
<td>eli</td>
<td>HTTP Server Type and Version</td>
<td>A web server is running on the remote host.</td>
<td>This plugin attempts to determine the type and the version of the remote web server.</td>
<td>The remote web server type is: cloudflare-nginx</td>
<td>n/a</td>
<td>Low/ CVSS2 Base Score: 1.0</td>
</tr>
</tbody>
</table>
### TCP 2095 nbx-ser 1.0

**Description:** HTTP Server Type and Version

**Synopsis:** A web server is running on the remote host.

**Impact:** This plugin attempts to determine the type and the version of the remote web server.

**Data Received:** The remote web server type is: cloudflare-nginx

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

### TCP 443 https 1.0

**Description:** SSL Certificate Information

**Synopsis:** This plugin displays the SSL certificate.

**Impact:** This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

**Data Received:** Subject Name:

- **Country:** US
- **State/Province:** CA
- **Locality:** San Francisco
- **Organization:** CloudFlare, Inc.
- **Common Name:** ssl7911.cloudflare.com

- **Issuer Name:**
  - **Country:** BE
  - **Organization:** GlobalSign nv-sa
  - **Common Name:** GlobalSign Organization Validation CA - G2

- **Serial Number:** 11 21 A2 10 5E EE FE 18 ED C2 67 CA BC 97 96 6F 42 37

- **Version:** 3

- **Signature Algorithm:** SHA-1 With RSA Encryption

- **Not Valid Before:** Oct 16 06:10:23 2014 GMT
- **Not Valid After:** Oct 17 06:10:23 2015 GMT

- **Public Key Info:**
  - **Algorithm:** RSA Encryption
  - **Key Length:** 2048 bits
  - **Key:** 00 BD C1 75 57 31 9A 6C 4B 0D 32 7E 86 A8 3D 7D A1 A1 ED B8 33 AE D3 E6 18 ED 5C 09 70 E2 22 11 5F 2D 37 77 90 46 9D 97 B3 DA E5 A1 A0 B2 63 7A E2 D2 7E F0 02 4A 90 5A 64 C9 14 B8 98 F0 08 C4 4C 66 B3 61 B1 B5 2D 20 8B 15 8C EE 22 8F 0F 7E A7 0F 93 8F A2 E6 B1 C9 67 FF 06 32 DE 72 22 2C 2C 75 E1 B5 E0 B4 02 D5 47 76 FA 7C 99 16 F9 34 15 4F 42 02 A7 A3 C4 59 3F D3 1A DC 1B 02 D9 E6 B2 D2 E6 50 59 35 60 55 3C 4D E2 2B E2 B9 DC 38 51 D9 F9 66 43 35 D5 E0 11 A5 F2 28 BD 17 9A B4 6C D7 7B 7B BA BE E0 C8 A8 06 B6 ED 0A 15 C9 40 50 03 B8 E7 4C E9 4A 39 7F 9C ED 9A 34 AC 29 12 F8 03 EC 1B 00 F0 EA 19 64 C1 03 C0 1B 9E 39 FF CE BD 4C 90 01 7D 65 65 AF 7B E5 7A A1 C2 B5 1A C0 13 75 D3 F7 40 46 E3 27 4C BA D7 43 EF 8D DF 94 06 F4 E9 F4 11 67 1F 29 4C C2 9D F4 22 C7 Exponent: 01 00 01

- **Signature Length:** 256 bytes / 2048 bits
- **Signature:** 00 05 88 44 A4 E8 F5 CE 2A CE 09 1D 65 CD 85 F8 90 FA D5 D4 E8 8F 65 CC 98 1D 78 43 E7 46 10 38 AE 4E 08 0A 80 7B 9A 5E 1C D9 3C 96 43 53 DC 90 62 EF 7F 4C E2 60 51 5E D0 7B A5 D8 0D 41 4B B7 0C 5B 5D 99 BC 23 26 D7 22 D2 2B A5 C2 DE 50 B8 54 B7 D7 E1 A7 8F 31 B8 8A B3 8A 9F AC F8 CF 05 DB 04 0D 80 BB CF C9 CA AD 89 3D D7 9F 58 3C 79 9E C2 4C OB 37 B6 D8 66 34 8E A6 B6 F8 F3 9C 48
**UDP**

**None**

**general**

**1.0**

**Description:** Traceroute Information

**Synopsis:** It was possible to obtain traceroute information.

**Impact:** Makes a traceroute to the remote host.

**Data Received:** For your information, here is the traceroute from 162.211.152.13 to 104.16.20.80:

```
162.211.152.13 162.211.152.1 74.122.79.37 128.177.104.245 64.125.20.237 64.125.26.5 64.125.12.194 62.115.32.214 104.16.20.80
```

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
<table>
<thead>
<tr>
<th>TCP</th>
<th>2083</th>
<th>radsec</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>HTTP Server Type and Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Synopsis:</strong></td>
<td>A web server is running on the remote host.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Impact:</strong></td>
<td>This plugin attempts to determine the type and the version of the remote web server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Received:</strong></td>
<td>The remote web server type is:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>cloudflare-nginx</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resolution:</strong></td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Factor:</strong></td>
<td>Low/ CVSS2 Base Score: 1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP</th>
<th>2082</th>
<th>infowave</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>HTTP Server Type and Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Synopsis:</strong></td>
<td>A web server is running on the remote host.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Impact:</strong></td>
<td>This plugin attempts to determine the type and the version of the remote web server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Received:</strong></td>
<td>The remote web server type is:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>cloudflare-nginx</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resolution:</strong></td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Factor:</strong></td>
<td>Low/ CVSS2 Base Score: 1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP</th>
<th>2087</th>
<th>eli</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>HyperText Transfer Protocol (HTTP) Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Synopsis:</strong></td>
<td>Some information about the remote HTTP configuration can be extracted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Impact:</strong></td>
<td>This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This test is informational only and does not denote any security problem.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Received:</strong></td>
<td>Protocol version: HTTP/1.1 SSL: no Keep-Alive: no Options allowed: (Not implemented) Headers:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server: cloudflare-nginx Date: Tue, 16 Jun 2015 09:55:15 GMT Content-Type: text/html Content-Length: 677 Connection: close</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resolution:</strong></td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Factor:</strong></td>
<td>Low/ CVSS2 Base Score: 1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Description:
SSL Cipher Block Chaining Cipher Suites Supported

### Synopsis:
The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

### Impact:
The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See also: [http://www.openssl.org/docs/apps/ciphers.html](http://www.openssl.org/docs/apps/ciphers.html)  
[http://www.nessus.org/u?cc4a822a](http://www.nessus.org/u?cc4a822a)  

### Data Received:
Here is the list of SSL CBC ciphers supported by the remote server: High Strength Ciphers (>= 112-bit key)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1</td>
<td>ECDHE-RSA-DES-CBC3-SHA</td>
<td>ECDH</td>
<td>RSA</td>
<td>3DES-CBC(168)</td>
<td>SHA1</td>
<td>RSA Enc=AES-CBC(128) Kx=ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1</td>
</tr>
<tr>
<td></td>
<td>ECDHE-RSA-AES128-SHA</td>
<td>ECDH</td>
<td>RSA</td>
<td>AES-CBC(128)</td>
<td>SHA1</td>
<td>RSA Enc=AES-CBC(256) Mac=SHA1</td>
</tr>
<tr>
<td></td>
<td>ECDHE-RSA-AES256-SHA</td>
<td>ECDH</td>
<td>RSA</td>
<td>AES-CBC(256)</td>
<td>SHA1</td>
<td>RSA Enc=AES-CBC(256) Mac=SHA1</td>
</tr>
<tr>
<td></td>
<td>RSA-AES128-SHA</td>
<td>RSA</td>
<td>RSA</td>
<td>AES-CBC(128)</td>
<td>SHA1</td>
<td>RSA Enc=AES-CBC(256) Mac=SHA1</td>
</tr>
<tr>
<td></td>
<td>RSA-AES256-SHA</td>
<td>RSA</td>
<td>RSA</td>
<td>AES-CBC(256)</td>
<td>SHA1</td>
<td>RSA Enc=AES-CBC(256) Mac=SHA1</td>
</tr>
</tbody>
</table>

The fields above are:

{OpenSSL ciphername} Kx={key exchange} Au={authentication} Enc={symmetric encryption method} Mac={message authentication code} {export flag}

### Resolution:
N/A

### Risk Factor:
Low/ CVSS2 Base Score: 1.0
### SSL Perfect Forward Secrecy Cipher Suites Supported

**Description:** SSL Perfect Forward Secrecy Cipher Suites Supported

**Synopsis:** The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

**Impact:** The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.


**Data Received:** Here is the list of SSL PFS ciphers supported by the remote server: High Strength Ciphers (>= 112-bit key)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cipher Suite</th>
<th>Key Exchange</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Message Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1</td>
<td>ECDHE-RSA-DES-CBC3-SHA</td>
<td>Kx=ECDH</td>
<td>Au=RSA</td>
<td>Enc=3DES-CBC(168) Mac=SHA1 ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1 ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1 ECDHE-RSA-AES128-SHA256 Kx=ECDHE Au=RSA Enc=AES-CBC(128) Mac=SHA256 ECDHE-RSA-AES256-SHA384 Kx=ECDHE Au=RSA Enc=AES-CBC(256) Mac=SHA384</td>
<td></td>
</tr>
<tr>
<td>TLSv12</td>
<td>ECDHE-RSA-AES128-SHA256</td>
<td>Kx=ECDHE</td>
<td>Au=RSA Enc=AES-GCM(128) Mac=SHA256 ECDHE-RSA-AES256-SHA384 Kx=ECDHE Au=RSA Enc=AES-GCM(256) Mac=SHA384</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

---

### HTTP Server Type and Version

**Description:** HTTP Server Type and Version

**Synopsis:** A web server is running on the remote host.

**Impact:** This plugin attempts to determine the type and the version of the remote web server.

**Data Received:** The remote web server type is:

cloudflare-nginx

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
**Description:** SSL Perfect Forward Secrecy Cipher Suites Supported

**Synopsis:** The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

**Impact:** The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See also: [http://www.openssl.org/docs/apps/ciphers.html](http://www.openssl.org/docs/apps/ciphers.html)  

**Data Received:** Here is the list of SSL PFS ciphers supported by the remote server: High Strength Ciphers (>= 112-bit key)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cipher Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1</td>
<td>ECDHE-RSA-DES-CBC3-SHA, Kx=ECDH, Au=RSA, Enc=3DES-CBC(168) Mac=SHA1 ECDHE-RSA-AES128-SHA, Kx=ECDH, Au=RSA, Enc=AES-CBC(128) Mac=SHA1 ECDHE-RSA-AES256-SHA, Kx=ECDH, Au=RSA, Enc=AES-CBC(256) Mac=SHA1 ECDHE-RSA-AES128-SHA256, Kx=ECDH, Au=RSA, Enc=AES-CBC(128) Mac=SHA256 ECDHE-RSA-AES256-SHA384, Kx=ECDH, Au=RSA, Enc=AES-CBC(256) Mac=SHA384</td>
</tr>
<tr>
<td>TLSv12</td>
<td>ECDHE-RSA-AES128-SHA256, Kx=ECDHE, Au=RSA, Enc=AES-GCM(128) Mac=SHA256 ECDHE-RSA-AES256-SHA384, Kx=ECDHE, Au=RSA, Enc=AES-GCM(256) Mac=SHA384</td>
</tr>
</tbody>
</table>

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

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
| Description: HyperText Transfer Protocol (HTTP) Information |
| Synopsis: Some information about the remote HTTP configuration can be extracted. |
| Impact: This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem. |
| Data Received: Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : (Not implemented) Headers : |
| Resolution: n/a |
| Risk Factor: Low/ CVSS2 Base Score: 1.0 |

<p>| Description: HyperText Transfer Protocol (HTTP) Information |
| Synopsis: Some information about the remote HTTP configuration can be extracted. |
| Impact: This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem. |
| Data Received: Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : (Not implemented) Headers : |
| Date: Tue, 16 Jun 2015 09:55:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache- Control: no-store, no-cache, must-revalidate, private, max-age=0 P3P: CP=&quot;ALL DSP COR CUR USD ADMa DEVa OUR IND COM NAV&quot; X-Rack-Cache: miss X-Request-Id: f5ce5837-6e474-438a-8fcb-3107e5ebf1c X-Runtime: 0.011875 Server: cloudflare-nginx CF-RAY: 1f759edd26432264-LAX |
| Resolution: n/a |
| Risk Factor: Low/ CVSS2 Base Score: 1.0 |</p>
<table>
<thead>
<tr>
<th>TCP</th>
<th>443</th>
<th>https</th>
<th>1.0</th>
</tr>
</thead>
</table>

**Description:** Web Server robots.txt Information Disclosure

**Synopsis:** The remote web server contains a `robots.txt` file.

**Impact:** The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See also:

http://www.robotstxt.org/wc/exclusion.html

**Data Received:** Contents of robots.txt:

```
# See http://www.robotstxt.org/wc/norobots.html for documentation on how to use the robots.txt file # The comments in here used to be funnier but since it shows up on UserVoice sites we thought we'd clean it up a bit. The original lives on at http://www.uservoice.com/robots.txt

# MSN bot is prone to over-crawling
User-agent: msnbot
Crawl-delay: 120

# YandexBot bot is prone to over-crawling
User-agent: YandexBot
Crawl-delay: 120

# 80legs is often abused
User-agent: 008
Disallow: /

# Disabled due to abuse
User-agent: TurnitinBot
Disallow: /

# Disabled due to abuse
User-agent: WBSearchBot
Disallow: /

# Disabled due to abuse
User-agent: SearchmetricsBot
Disallow: /

Other references: OSVDB:238
```

**Resolution:** Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

<table>
<thead>
<tr>
<th>TCP</th>
<th>443</th>
<th>https</th>
<th>1.0</th>
</tr>
</thead>
</table>

**Description:** SSL / TLS Versions Supported

**Synopsis:** The remote service encrypts communications.

**Impact:** This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

**Data Received:** This port supports TLSv1.0/TLSv1.1/TLSv1.2.

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Service</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>2096</td>
<td>nbx-dir</td>
<td>1.0</td>
</tr>
<tr>
<td>TCP</td>
<td>2053</td>
<td>lot105-ds-upd</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Description:** HyperText Transfer Protocol (HTTP) Information

**Synopsis:** Some information about the remote HTTP configuration can be extracted.

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

This test is informational only and does not denote any security problem.

**Data Received:**
- Protocol version: HTTP/1.1
- SSL: no
- Keep-Alive: no
- Options allowed: (Not implemented)
- Headers:
  - Server: cloudflare-nginx
  - Date: Tue, 16 Jun 2015 09:56:15 GMT
  - Content-Type: text/html
  - Content-Length: 677
  - Connection: close

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

**Description:** HTTP Server Type and Version

**Synopsis:** A web server is running on the remote host.

**Impact:** This plugin attempts to determine the type and the version of the remote web server.

**Data Received:** The remote web server type is:
- cloudflare-nginx

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Service</th>
<th>Version</th>
<th>Description</th>
<th>Synopsis</th>
<th>Impact</th>
<th>Data Received</th>
<th>Resolution</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>8080</td>
<td>http-alt</td>
<td>1.0</td>
<td><strong>Description:</strong> HyperText Transfer Protocol (HTTP) Information</td>
<td><strong>Synopsis:</strong> Some information about the remote HTTP configuration can be extracted.</td>
<td><strong>Impact:</strong> This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem.</td>
<td>Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : (Not implemented) Headers : Date: Tue, 16 Jun 2015 09:57:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache X-Frame-Options: SAMEORIGIN Server: cloudflare-nginx CF-RAY: 1f75a5ebdd7920fc-LAX</td>
<td>n/a</td>
<td>Low/ CVSS2 Base Score: 1.0</td>
</tr>
</tbody>
</table>

<p>| TCP      | None | general | 1.0     | <strong>Description:</strong> Additional DNS Hostnames                          | <strong>Synopsis:</strong> Potential virtual hosts have been detected. | <strong>Impact:</strong> Hostnames different from the current hostname have been collected by miscellaneous plugins. Different web servers may be hosted on name-based virtual hosts. | See also : <a href="http://en.wikipedia.org/wiki/Virtual_hosting">http://en.wikipedia.org/wiki/Virtual_hosting</a> | The following hostnames point to the remote host: - uservoice.com | If you want to test them, re-scan using the special vhost syntax, such as : <a href="http://www.example.com%5B192.0.32.10">www.example.com[192.0.32.10</a>] | Low/ CVSS2 Base Score: 1.0 |</p>
<table>
<thead>
<tr>
<th>TCP</th>
<th>2052</th>
<th>clearvisn</th>
<th>1.0</th>
</tr>
</thead>
</table>

**Description:** HyperText Transfer Protocol (HTTP) Information

**Synopsis:** Some information about the remote HTTP configuration can be extracted.

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

This test is informational only and does not denote any security problem.

**Data Received:**
- Protocol version: HTTP/1.1
- SSL: no
- Keep-Alive: no
- Options allowed: (Not implemented)
- Headers:
  - Date: Tue, 16 Jun 2015 09:53:13 GMT
  - Content-Type: text/html; charset=UTF-8
  - Transfer-Encoding: chunked
  - Connection: keep-alive
  - Expires: Thu, 01 Jan 1970 00:00:01 GMT
  - Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  - Pragma: no-cache
  - X-Frame-Options: SAMEORIGIN
  - Server: cloudflare-nginx
  - CF-RAY: 1f759ffe87121431-LAX

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
**Description:** Web Server robots.txt Information Disclosure

**Synopsis:** The remote web server contains a 'robots.txt' file.

**Impact:** The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See also:

http://www.robotstxt.org/wc/exclusion.html

**Data Received:** Contents of robots.txt:

```text
# See http://www.robotstxt.org/wc/norobots.html for documentation on how to use the robots.txt file
# The comments in here used to be funnier but since it shows up on UserVoice sites we thought we'd clean it up a bit. The original lives on at http://www.uservoice.com/robots.txt

# MSN bot is prone to over-crawling
User-agent: msnbot
Crawl-delay: 120

# YandexBot bot is prone to over-crawling
User-agent: YandexBot
Crawl-delay: 120

# 80legs is often abused
User-agent: 008
Disallow: /

# Disabled due to abuse
User-agent: TurnitinBot
Disallow: /

User-agent: WBSearchBot
Disallow: /

User-agent: SearchmetricsBot
Disallow: /

Other references: OSVDB:238
```

**Resolution:** Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
<table>
<thead>
<tr>
<th>TCP</th>
<th>2083</th>
<th>radsec</th>
<th>1.0</th>
</tr>
</thead>
</table>

**Description:** HyperText Transfer Protocol (HTTP) Information

**Synopsis:** Some information about the remote HTTP configuration can be extracted.

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

This test is informational only and does not denote any security problem.

**Data Received:** Protocol version: HTTP/1.1 SSL: no Keep-Alive: no Options allowed: (Not implemented) Headers:

- Server: cloudflare-nginx
- Date: Tue, 16 Jun 2015 09:54:14 GMT
- Content-Type: text/html
- Content-Length: 677
- Connection: close

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
**Description:** SSL Cipher Suites Supported

**Synopsis:** The remote service encrypts communications using SSL.

**Impact:** This script detects which SSL ciphers are supported by the remote service for encrypting communications.

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

**Data Received:** Here is the list of SSL ciphers supported by the remote server:

- Each group is reported per SSL Version.

<table>
<thead>
<tr>
<th>SSL Version</th>
<th>High Strength Ciphers (&gt;= 112-bit key)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv12</td>
<td>ECDHE-RSA-DES-CBC3-SHA Kx=ECDH Au=RSA Enc=3DES-CBC(168) Mac=SHA1 ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1 ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1 DES-CBC3-SHA Kx=RSA Enc=3DES-CBC(168) Mac=SHA1 AES128-SHA Kx=RSA Enc=AES-CBC(128) Mac=SHA1 AES256-SHA Kx=RSA Enc=AES-CBC(256)</td>
</tr>
<tr>
<td>TLSv11</td>
<td>ECDHE-RSA-DES-CBC3-SHA Kx=ECDH Au=RSA Enc=3DES-CBC(168) Mac=SHA1 ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1 ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1 DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1 AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1 AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ECDHE-RSA-DES-CBC3-SHA Kx=ECDH Au=RSA Enc=3DES-CBC(168) Mac=SHA1 ECDHE-RSA-AES128-SHA Kx=ECDH Au=RSA Enc=AES-CBC(128) Mac=SHA1 ECDHE-RSA-AES256-SHA Kx=ECDH Au=RSA Enc=AES-CBC(256) Mac=SHA1 DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1 AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1 AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1</td>
</tr>
</tbody>
</table>

The fields above are:


**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
**Description:** TLS Next Protocols Supported

**Synopsis:** The remote service advertises one or more protocols as being supported over TLS.

**Impact:** This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that SecurityMetrics did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and/or failing to advertise other supported protocols.

See also: http://tools.ietf.org/html/draft-agl-tls-nextprotoneg
https://technotes.googlecode.com/git/nextprotoneg.html

**Data Received:** The target advertises that the following protocols are supported over SSL/TLS:

http/1.1 spdy/3.1

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

---

**Description:** SSL Certificate Information

**Synopsis:** This plugin displays the SSL certificate.

**Impact:** This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

**Data Received:** Subject Name:

Country: US State/Province: CA Locality: San Francisco Organization: CloudFlare, Inc. Common Name: ssl7911.cloudflare.com Issuer Name:

Country: BE Organization: GlobalSign nv-sa Common Name: GlobalSign Organization Validation CA - G2

Serial Number: 11 21 A2 10 5E EE FE 18 ED C2 67 CA BC 97 96 6F 42 37

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption


Public Key Info: Algorithm: RSA Encryption Key Length: 2048 bits Public Key: 00 BD C1 75 57 31 9A C6 4B 0D 32 7E 86 A8 3D 7D A1 A1 ED 88 33 AE D3 E6 18 ED 5C 09 70 E2 22 11 5F 2D 37 77 90 46 9D 97 B3 DA E5 A1 A0 82 63 7A E2 D2 7E F0 02 4A 90 5A 64 C9 14 B8 98 F0 08 C4 4C 65 C2 86 B3 61 B1 B5 2D 20 8B 15 8C EE 22 8F 0F 7E A7 0F 93 8F A2 E6 B1 C9 67 FF 06 32 DE 72 22 2C 2C 75 E1 B5 E0 B4 02 D5 47 76 FA 7C 99 16 F9 34 15 4F 42 02 A7 A3 C4 59 3F D3 1A DC 1B 02 D9 E6 B2 D2 E6 50 59 35 60 55 3C 4D E2 2B E2 B9 DC 38 51 D9 F9 66 43 35 D5 E0 11 A5 F2 2B BD 17 9A B4 6C D7 7B 7B BA BE E0 C8 A8 06 B6 ED 0A 15 C9 40 50 03 B8 E7 4C E9 4A 39 7F 9C ED 9A 34 AC 29 12 FB 03 EC 1B 00 F0 EA 19 64 C1 03 C0 1B 9E 39 FF CE BD 4C 90 01 7D 65
<table>
<thead>
<tr>
<th>Extension: Key Usage (2.5.29.15) Critical: 1 Key Usage: Digital Signature, Key Encipherment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension: Policies (2.5.29.32) Critical: 0 Policy ID #1: 2.23.140.1.2.2 Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1) CPS URI: <a href="https://www.globalsign.com/repository/">https://www.globalsign.com/repository/</a></td>
</tr>
<tr>
<td>Extension: Subject Alternative Name (2.5.29.17) Critical: 0 DNS: ssl7911.cloudflare.com DNS: *.uservoice.com DNS: uservoice.com</td>
</tr>
<tr>
<td>Extension: Basic Constraints (2.5.29.19) Critical: 0</td>
</tr>
<tr>
<td>Extension: Extended Key Usage (2.5.29.37) Critical: 0 Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1) Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)</td>
</tr>
<tr>
<td>Extension: CRL Distribution Points (2.5.29.31) Critical: 0 URI: <a href="http://crl.globalsign.com/gs/gsorganizationvalg2.crl">http://crl.globalsign.com/gs/gsorganizationvalg2.crl</a></td>
</tr>
<tr>
<td>Extension: Subject Key Identifier (2.5.29.14) Critical: 0 Subject Key Identifier: 4F D9 6A D8 FE 86 FA 02 09 3B 5D A1 0C F1 70 8B 4F 71 7F 3E</td>
</tr>
<tr>
<td>Extension: Authority Key Identifier (2.5.29.35) Critical: 0 Key Identifier: 5D 46 B2 8D C4 4B 74 1C BB ED F5 73 B6 3A B7 38 8F 75 9E 7E</td>
</tr>
<tr>
<td>Resolution: n/a</td>
</tr>
<tr>
<td>Risk Factor: Low/ CVSS2 Base Score: 1.0</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>TCP</td>
</tr>
</tbody>
</table>

**Description:** HTTP Server Type and Version

**Synopsis:** A web server is running on the remote host.

**Impact:** This plugin attempts to determine the type and the version of the remote web server.

**Data Received:** The remote web server type is:

cloudflare-nginx

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

**Description:** HTTP Server Type and Version

**Synopsis:** A web server is running on the remote host.

**Impact:** This plugin attempts to determine the type and the version of the remote web server.

**Data Received:** The remote web server type is:

cloudflare-nginx

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

**Description:** HyperText Transfer Protocol (HTTP) Information

**Synopsis:** Some information about the remote HTTP configuration can be extracted.

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

This test is informational only and does not denote any security problem.

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


**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service</th>
<th>Description</th>
<th>Synopsis</th>
<th>Impact</th>
<th>Data Received</th>
<th>Resolution</th>
<th>Risk Factor</th>
<th>CVSS2 Base Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 8443</td>
<td>TCP</td>
<td>pcsync-https</td>
<td><strong>Description:</strong> SSL / TLS Versions Supported</td>
<td><strong>Synopsis:</strong> The remote service encrypts communications.</td>
<td><strong>Impact:</strong> This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.</td>
<td><strong>Data Received:</strong> This port supports TLSv1.0/TLSv1.1/TLSv1.2.</td>
<td>n/a</td>
<td>Low/</td>
<td>1.0</td>
</tr>
<tr>
<td>TCP 2053</td>
<td>TCP</td>
<td>lot105-ds-upd</td>
<td><strong>Description:</strong> HyperText Transfer Protocol (HTTP) Information</td>
<td><strong>Synopsis:</strong> Some information about the remote HTTP configuration can be extracted.</td>
<td><strong>Impact:</strong> This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...</td>
<td><strong>Data Received:</strong> Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : (Not implemented) Headers :</td>
<td>n/a</td>
<td>Low/</td>
<td>1.0</td>
</tr>
<tr>
<td>TCP</td>
<td>TCP</td>
<td>general</td>
<td><strong>Description:</strong> Host Fully Qualified Domain Name (FQDN) Resolution</td>
<td><strong>Synopsis:</strong> It was possible to resolve the name of the remote host.</td>
<td><strong>Impact:</strong> SecurityMetrics was able to resolve the FQDN of the remote host.</td>
<td><strong>Data Received:</strong> 104.16.20.80 resolves as app.uservoice.com.</td>
<td>n/a</td>
<td>Low/</td>
<td>1.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Port</td>
<td>Vendor</td>
<td>Version</td>
<td>Description</td>
<td>Synopsis</td>
<td>Impact</td>
<td>Data Received</td>
<td>Resolution</td>
<td>Risk Factor</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>TCP</td>
<td>2052</td>
<td>clearvis</td>
<td>1.0</td>
<td><strong>Description:</strong> HTTP Server Type and Version</td>
<td><strong>Synopsis:</strong> A web server is running on the remote host.</td>
<td><strong>Impact:</strong> This plugin attempts to determine the type and the version of the remote web server.</td>
<td><strong>Data Received:</strong> The remote web server type is: cloudflare-nginx</td>
<td>n/a</td>
<td>Low/ CVSS2 Base Score: 1.0</td>
</tr>
</tbody>
</table>
| TCP      | 2095 | nbx-ser  | 1.0     | **Description:** HyperText Transfer Protocol (HTTP) Information               | **Synopsis:** Some information about the remote HTTP configuration can be extracted. | **Impact:** This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... | **Data Received:** Protocol version : HTTP/1.1 SSL : no Keep-Alive : no Options allowed : (Not implemented) Headers :  
Date: Tue, 16 Jun 2015 09:56:15 GMT Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked Connection: keep-alive Expires: Thu, 01 Jan 1970 00:00:01 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache  
X-Frame-Options: SAMEORIGIN  
Server: cloudflare-nginx CF-RAY: 1f75a47018c10369-LAX | n/a        | Low/ CVSS2 Base Score: 1.0                                                  |
### TCP 2082 infowave 1.0

**Description:** HyperText Transfer Protocol (HTTP) Information

**Synopsis:** Some information about the remote HTTP configuration can be extracted.

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

This test is informational only and does not denote any security problem.

**Data Received:**
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)

Headers :

- Date: Tue, 16 Jun 2015 09:54:14 GMT
- Content-Type: text/html; charset=UTF-8
- Transfer-Encoding: chunked
- Connection: keep-alive
- Expires: Thu, 01 Jan 1970 00:00:01 GMT
- Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
-Pragma: no-cache
- X-Frame-Options: SAMEORIGIN
- Server: cloudflare- nginx
- CF-RAY: 1f75a17991550369-LAX

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0

---

### TCP 8443 pcsync-https 1.0

**Description:** TLS Next Protocols Supported

**Synopsis:** The remote service advertises one or more protocols as being supported over TLS.

**Impact:** This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that SecurityMetrics did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See also:
- https://technotes.googlecode.com/git/nextprotneg.html

**Data Received:** The target advertises that the following protocols are supported over SSL / TLS :

- http/1.1
- spdy/3.1

**Resolution:** n/a

**Risk Factor:** Low/ CVSS2 Base Score: 1.0
This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-10, within the guidelines of the PCI data security initiative.