Nessus Report

Nessus Scan Report

17/May/2015:12:47:29

Nessus Home: Commercial use of the report is prohibited

Table Of Contents

Vulnerabilities By Plugin

26194 (1) - Web Server Uses Plain Text Authentication Forms

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information:

Publication date: 2007/09/28, Modification date: 2014/12/30

Hosts

192.168.1.50 (tcp/80)

```
Page : /
Destination Page: /login

Page : /login
Destination Page: /login
```

70658 (1) - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Publication date: 2013/10/28, Modification date: 2014/01/28

Hosts

192.168.1.50 (tcp/22)

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

71049 (1) - SSH Weak MAC Algorithms Enabled

Synopsis

SSH is configured to allow MD5 and 96-bit MAC algorithms.

Description

The SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2013/11/22, Modification date: 2014/07/08

Hosts

192.168.1.50 (tcp/22)

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
```

14272 (13) - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2014/05/23

Hosts

192.168.1.50 (tcp/22)

```
Port 22/tcp was found to be open
```

192.168.1.50 (tcp/80)

```
Port 80/tcp was found to be open
```

192.168.1.50 (udp/500)

```
Port 500/udp was found to be open
```

192.168.1.50 (udp/514)

```
Port 514/udp was found to be open
```

192.168.1.50 (udp/3503)

```
Port 3503/udp was found to be open
```

192.168.1.50 (udp/3784)

```
Port 3784/udp was found to be open
```

192.168.1.50 (udp/4500)

```
Port 4500/udp was found to be open
```

192.168.1.50 (udp/4784)

```
Port 4784/udp was found to be open
```

192.168.1.50 (udp/6333)

```
Port 6333/udp was found to be open
```

192.168.1.50 (udp/31342)

```
Port 31342/udp was found to be open
```

192.168.1.50 (udp/49152)

```
Port 49152/udp was found to be open
```

192.168.1.50 (udp/57708)

```
Port 57708/udp was found to be open
```

192.168.1.50 (udp/65062)

```
Port 65062/udp was found to be open
```

22964 (2) - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2015/05/14

Hosts

192.168.1.50 (tcp/22)

```
An SSH server is running on this port.
```

192.168.1.50 (tcp/80)

```
A web server is running on this port.
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2014/08/01

Hosts

192.168.1.50 (tcp/80)

```
The remote web server type is :

Embedthis-Appweb/3.2.3
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Hosts

192.168.1.50 (icmp/0)

```
The difference between the local and remote clocks is 34863 seconds.
```

10267 (1) - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2015/03/26

Hosts

192.168.1.50 (tcp/22)

```
SSH version : SSH-2.0-OpenSSH_6.6
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Hosts

192.168.1.50 (udp/0)

```
For your information, here is the traceroute from 192.168.1.57 to 192.168.1.50 :
192.168.1.57
192.168.1.50
```

10662 (1) - Web mirroring

Synopsis

Nessus crawled the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2015/05/08

Hosts

192.168.1.50 (tcp/80)

```
Webmirror performed 10 queries in 3s (3.0333 queries per second)

The following CGIs have been discovered :


+ CGI : /login
  Methods : POST
  Argument : login
   Value: login
  Argument : password
  Argument : username
```

10881 (1) - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/06, Modification date: 2013/10/21

Hosts

192.168.1.50 (tcp/22)

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g. TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also sometimes possible to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2015/05/12

Hosts

192.168.1.50 (tcp/0)

```
Remote operating system : Juniper Junos Version 12.1X47-D20.7
Confidence level : 100
Method : uname


The remote host is running Juniper Junos Version 12.1X47-D20.7
```

12634 (1) - Authenticated Check : OS Name and Installed Package Enumeration

Synopsis

This plugin gathers information about the remote host via an authenticated session.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet, or local commands and extracts the list of installed packages.
If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/07/06, Modification date: 2015/05/12

Hosts

192.168.1.50 (tcp/0)

```
It was possible to log into the remote host using the supplied
password.

Local security checks have been enabled for Juniper Junos.
```

19506 (1) - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of scanner (Nessus or Nessus Home)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2015/01/20

Hosts

192.168.1.50 (tcp/0)

```
Information about this scan :

Nessus version : 6.3.6
Plugin feed version : 201505161915
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.57
Port scanner(s) : netstat
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'root' via ssh
Patch management checks : None
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2015/5/17 12:37 CET
Scan duration : 615 sec
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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 sometimes be computed.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Hosts

192.168.1.50 (tcp/0)

33817 (1) - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/26, Modification date: 2014/03/12

Hosts

192.168.1.50 (tcp/80)

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

format string                           : S=6          SP=14        AP=14        SC=16
 AC=16
arbitrary command execution (time based) : S=18         SP=42        AP=42        SC=48
 AC=48
cross-site scripting (comprehensive test): S=12         SP=28        AP=28        SC=32
 AC=32
injectable parameter                    : S=6          SP=14        AP=14        SC=16
 AC=16
directory traversal                     : S=75         SP=175       AP=175       SC=200
 AC=200
local file inclusion                    : S=3          SP=7         AP=7         SC=8
 AC=8
arbitrary command execution             : S=48         SP=112       AP=112       SC=128
 AC=128
web code injection                      : S=3          SP=7         AP=7         SC=8
 AC=8
blind SQL injection (4 requests)        : S=12         SP=28        AP=28        SC=32
 AC=32
directory traversal (write access)      : S=6          SP=14        AP=14        SC=16
 AC=16
persistent XSS                          : S=12         SP=28        AP=28        SC=32
 AC=32
XML injection                           : S=3          SP=7         AP=7         SC=8
 AC=8
blind SQL injection                     : S=36         SP=84        AP=84        SC=96
 AC=96
directory traversal (extended test)     : S=153        SP=357       AP=357       SC=408
 AC=408
SQL injection (2nd order)               : S=3          SP=7         AP=7         SC=8
 AC=8
SSI injection                           : S=9          SP=21        AP=21        SC=24
 AC=24
SQL injection                           : S=72         SP=168       AP=168       SC=192
 AC=192
unseen parameters                      [...]
```

35716 (1) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'.
These OUI are registered by IEEE.

See Also

http://standards.ieee.org/faqs/OUI.html

http://standards.ieee.org/regauth/oui/index.shtml

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2011/03/27

Hosts

192.168.1.50 (tcp/0)

```
The following card manufacturers were identified :

08:00:27:ed:ae:dc : CADMUS COMPUTER SYSTEMS
```

39470 (1) - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan.
The results may be incomplete.

Solution

Consider increasing the 'maximum run time (min)' preference for the 'Web Application Tests Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :
- Combinations of arguments values = 'all combinations' is much slower than 'two pairs' or 'single'.
- Stop at first flaw = 'per port' is quicker.
- In 'some pairs' or 'some combinations' mode, try reducing web_app_tests.tested_values_for_each_parameter in nessusd.conf

Risk Factor

None

Plugin Information:

Publication date: 2009/06/19, Modification date: 2014/03/10

Hosts

192.168.1.50 (tcp/80)

```
The following tests timed out without finding any flaw :
- SQL injection
```

40406 (1) - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :
- Network -> Network Receive Timeout (check_read_timeout)
- Options -> Number of hosts in parallel (max_hosts)
- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information:

Publication date: 2009/07/28, Modification date: 2011/09/21

Hosts

192.168.1.50 (tcp/80)

```
Nessus encountered :

  - 1 error involving SQL injection (on parameters names) checks :
   . reading the status line: errno=2 (connection reset by peer)
  - 1 error involving XSS (on parameters names) checks :
   . reading the status line: errno=2 (connection reset by peer)
```

40773 (1) - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.
** This plugin only reports information that may be useful for auditors
** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information:

Publication date: 2009/08/25, Modification date: 2012/08/17

Hosts

192.168.1.50 (tcp/80)

```
Potentially sensitive parameters for CGI /login :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

43111 (1) - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Hosts

192.168.1.50 (tcp/80)

```
Based on the response to an OPTIONS request :

  - HTTP methods DELETE GET HEAD OPTIONS POST PUT are allowed on :

    /
    /extjs
    /extjs/resources
    /extjs/resources/css
    /images
    /stylesheet
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/11/20

Hosts

192.168.1.50 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:juniper:junos:12.1x47 -> Juniper JUNOS 12.1X47

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH 6.6
```

49704 (1) - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Hosts

192.168.1.50 (tcp/80)

```
3 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://www.juniper.net/footer
       legal.html - /
http://www.juniper.net/footerlegal.html#05 - /
http://www.juniper.net/privacy.html     - /
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Hosts

192.168.1.50 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 100
```

55932 (1) - Junos Version Detection

Synopsis

It is possible to obtain the operating system version number of the remote Juniper device.

Description

The remote host is running Junos, an operating system for Juniper devices.
It is possible to read the Junos version number by logging into the device via SSH, using SNMP, or viewing the web interface.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/08/22, Modification date: 2014/03/06

Hosts

192.168.1.50 (tcp/0)

```
Junos version : 12.1X47-D20.7
Build date    : 2015-03-03
Model         : FIREFLY-PERIMETER
Source        : SSH
```

56468 (1) - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/10/12, Modification date: 2014/07/25

Hosts

192.168.1.50 (tcp/0)

```
2015-05-17 09:40:02 UTC
```

58651 (1) - Netstat Active Connections

Synopsis

Active connections are enumerated via the 'netstat' command.

Description

This plugin runs 'netstat' on the remote machine to enumerate all active 'ESTABLISHED' or 'LISTENING' tcp/udp connections.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/04/10, Modification date: 2012/04/10

Hosts

192.168.1.50 (tcp/0)

```
Netstat output :
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address                                    Foreign Address
             (state)
tcp4       0      0  192.168.1.50.22                                  192.168.1.57.55709
             ESTABLISHED
tcp4       0      0  *.33088                                          *.*
             LISTEN
tcp4       0      0  128.0.0.1.33040                                  128.0.0.1.63620
             ESTABLISHED
tcp4       0      0  128.0.0.1.63620                                  128.0.0.1.33040
             ESTABLISHED
tcp4       0      0  *.33039                                          *.*
             LISTEN
tcp4       0      0  128.0.0.1.33067                                  128.0.0.1.60036
             ESTABLISHED
tcp4       0      0  128.0.0.1.60036                                  128.0.0.1.33067
             ESTABLISHED
tcp4       0      0  *.33066                                          *.*
             LISTEN
tcp4       0      0  128.0.0.1.33075                                  128.0.0.1.63596
             ESTABLISHED
tcp4       0      0  128.0.0.1.63596                                  128.0.0.1.33075
             ESTABLISHED
tcp4       0      0  *.32032                                          *.*
             LISTEN
tcp4       0      0  *.6156                                           *.*
             LISTEN
tcp4       0      0  128.0.1.16.6160                                  *.*
             LISTEN
tcp4       0      0  *.666                                            *.*
             LISTEN
tcp4       0      0  128.0.1.16.6154                                  *.*
             LISTEN
tcp4       0      0  128.0. [...]
```

64582 (1) - Netstat Connection Information

Synopsis

Nessus is able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/02/13, Modification date: 2013/06/18

Hosts

192.168.1.50 (tcp/0)

```
tcp4 (established)
  src: [host=192.168.1.50, port=22]
  dst: [host=192.168.1.57, port=55709]

tcp4 (listen)
  src: [host=*, port=33088]
  dst: [host=*, port=*]

tcp4 (established)
  src: [host=128.0.0.1, port=33040]
  dst: [host=128.0.0.1, port=63620]

tcp4 (established)
  src: [host=128.0.0.1, port=63620]
  dst: [host=128.0.0.1, port=33040]

tcp4 (listen)
  src: [host=*, port=33039]
  dst: [host=*, port=*]

tcp4 (established)
  src: [host=128.0.0.1, port=33067]
  dst: [host=128.0.0.1, port=60036]

tcp4 (established)
  src: [host=128.0.0.1, port=60036]
  dst: [host=128.0.0.1, port=33067]

tcp4 (listen)
  src: [host=*, port=33066]
  dst: [host=*, port=*]

tcp4 (established)
  src: [host=128.0.0.1, port=33075]
  dst: [host=128.0.0.1, port=63596]

tcp4 (established)
  src: [host=128.0.0.1, port=63596]
  dst: [host=128.0.0.1, port=33075]

tcp4 (listen)
  src: [host=*, port=32032]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=6156]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=128.0.1.16, port=6160]
  dst: [host=*, port=*]
```

```
tcp4 (listen)
  src: [host=*, port=666]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=128.0.1.16, port=6154]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=128.0.1.16, port=6200]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=33151]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=33064]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=33152]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=33067]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=33040]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=6161]
  dst: [host=*, port=*]

tcp4 (established)
  src: [host=128.0.0.4, port=9000]
  dst: [host=128.0.0.4, port=54611]

tcp4 (established)
  src: [host=128.0.0.4, port=54611]
  dst: [host=128.0.0.4, port=9000]

tcp4 (listen)
  src: [host=*, port=51627]
  dst: [host=*, port=*]

tcp46 (listen)
  src: [host=*, port=80]
  dst: [host=*, port=*]

tcp4 (listen)
  src: [host=*, port=80]
  dst: [host=*, port=*]
 [...]
```

70657 (1) - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2014/04/04

Hosts

192.168.1.50 (tcp/22)

```
Nessus negotiated the following encryption algorithm with the server : aes128-cbc

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
```

```
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.c [...]
```