



RK3 loc off to online

Report generated by Nessus™

Tue, 06 Jul 2021 10:04:34 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 30.90.90.145.....4

Vulnerabilities by Host

30.90.90.145



Scan Information

Start time: Tue Jul 6 09:47:16 2021
End time: Tue Jul 6 10:04:34 2021

Host Information

IP: 30.90.90.145
OS: CISCO PIX 7.0

Vulnerabilities

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	2112
CVE	CVE-1999-0517

Plugin Information

Published: 2002/11/25, Modified: 2018/08/22

Plugin Output

udp/161/snmp

```
The remote SNMP server replies to the following default community
string :

public
```

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2009/10/27, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Nessus collected the following banner from the remote Telnet server :
```

```
----- snip -----
*****
* Welcome to telnet_debug                               *
* built-ins are:                                         *
  help -- Itemizes the available commands.
  exit  -- Terminates this telnet session.
  quit  -- Terminates this telnet session.
  pwd   -- Display current working directory.
  ls    -- List commands and directories.
```

```
cd -- Reset current working directory.  
*****  
telnet_debug>  
----- snip -----
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was 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/>

<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/06/03

Plugin Output

tcp/0

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

```
cpe:/o:cisco:pix_firewall:7.0
```


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

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : firewall  
Confidence level : 70
```

10107 - 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

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :
```

```
Mrvl-Rl_0
```

10107 - 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

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/631/www

```
The remote web server type is :  
  
Mrv1-R1_0
```

10107 - 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

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8080/www

```
The remote web server type is :
```

```
Mrvl-Rl_0
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/0

```
Nessus SNMP scanner was able to retrieve the open port list
with the community name: p*****
It found 8 open TCP ports and 2 open UDP ports.
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/23/telnet

```
Port 23/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/80/www

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

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/137

```
Port 137/udp was found to be open
```


Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/515

```
Port 515/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/631/www

```
Port 631/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/3910

```
Port 3910/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/3911

```
Port 3911/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8080/www

```
Port 8080/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/9100/jetdirect

```
Port 9100/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/45938

```
Port 45938/udp was found to be open
```

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin 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.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- 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

Published: 2005/08/26, Modified: 2021/01/27

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 8.14.0
Plugin feed version : 202106121427
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : rubber kin
Scanner IP : 192.168.58.131
Port scanner(s) : snmp_scanner
Port range : 0-65535
```



```
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/6 9:47 EDT
Scan duration : 1033 sec
```

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 possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2021/05/12

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0  
Confidence level : 70  
Method : SinFP
```

```
The remote host is running CISCO PIX 7.0
```

25037 - Printer Job Language (PJP) Detection

Synopsis

The remote host uses the PJP protocol.

Description

Nessus had detected that the service running on the remote host will answer an HP Printer Job Language (PJP) request, which indicates that it is a printer device running HP JetDirect. By using the PJP protocol, users can submit printing jobs, transfer files to or from the printer, and change configuration settings.

See Also

<http://www.maths.usyd.edu.au/u/psz/ps.html>

<http://www.nessus.org/u?92cb3210>

<http://h10032.www1.hp.com/ctg/Manual/bpl13208>

<http://h10032.www1.hp.com/ctg/Manual/bpl13207>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/04/14, Modified: 2020/01/22

Plugin Output

tcp/9100/jetdirect

The device INFO ID is:

HP LaserJet Professional P1606dn

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/31, Modified: 2013/01/19

Plugin Output

udp/161/snmp

```
This host supports SNMP version SNMPv1.  
This host supports SNMP version SNMPv2c.
```

Synopsis

The remote service could be identified.

Description

Nessus was able 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

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/80/www

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

Synopsis

The remote service could be identified.

Description

Nessus was able 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

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/631/www

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

Synopsis

The remote service could be identified.

Description

Nessus was able 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

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/8080/www

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

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Here is the banner from the remote Telnet server :
```

```
----- snip -----
*****
* Welcome to telnet_debug                                     *
* built-ins are:                                           *
  help -- Itemizes the available commands.
  exit -- Terminates this telnet session.
  quit -- Terminates this telnet session.
  pwd  -- Display current working directory.
  ls   -- List commands and directories.
  cd   -- Reset current working directory.
*****
telnet_debug>
----- snip -----
```


Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.58.131 to 30.90.90.145 :  
192.168.58.131  
192.168.58.2  
30.90.90.145  
  
Hop Count: 2
```