Scan Report

December 10, 2018

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "router.rz.lab - External OpenVAS Scan - Deep Probe". The scan started at Sun Dec 9 22:07:42 2018 UTC and ended at Sun Dec 9 22:39:57 2018 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
172.29.167.179 router.mshome.net	0	2	1	23	1
Total: 1	0	2	1	23	1

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 27 results selected by the filtering described above. Before filtering there were 27 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
172.29.167.179 - router.mshome.net	SSH	Success	Protocol SSH, Port 22, User vagrant

2 Results per Host

2.1 172.29.167.179

Host scan start Sun Dec 9 22:07:54 2018 UTC
Host scan end Sun Dec 9 22:39:57 2018 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Low
80/tcp	Log
general/HOST-T	Log
general/CPE-T	Log
general/tcp	Log
general/icmp	Log
22/tcp	Log
general/tcp	False Positive

2.1.1 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: `$Revision: 12308 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2018-15919`

. . . continues on next page . . .

... continued from previous page ...

```
Other:
  URL:http://www.openssh.com
   URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
   URL:https://seclists.org/oss-sec/2018/q3/180
```

Note

```
Ubuntu 18.04 currently does not have a vendor supported update to install OpenSS
↪H 7.9 or greater.
Accepted Risk.
```

Last modified: Sun Dec 9 18:39:42 2018 UTC

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result

```
cpe:/a:openbsd:openssh:7.6p1
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

Summary

This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result

```
Installed version: 7.6p1
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact

Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution

Solution type: NoneAvailable

No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS

OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH User Enumeration Vulnerability-Aug18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15473
Other:
  URL:http://www.openssh.com
   URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

Note

```
Ubuntu 18.04 currently does not have a vendor supported update to install OpenSS
↪H 7.9 or greater.
Accepted Risk.
```

Last modified: Sun Dec 9 18:38:21 2018 UTC

[return to 172.29.167.179]

2.1.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
```

... continues on next page ...

... continued from previous page ...

```
Packet 1: 4176619188
Packet 2: 4176620195
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 10411 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 172.29.167.179]

2.1.3 Log 80/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

... continues on next page ...

... continued from previous page ...

- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of these are wrong please report to https://community.greenbone.net/c/vulnerability-tests.

Vulnerability Detection Result

```
The Hostname/IP "router.mshome.net" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; GBN-VT 9.0.3)" was used to access the
↪remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://router.mshome.net/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 11638 $

Log (CVSS: 0.0)
NVT: Services

Summary

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

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

Log Method

Details: Services

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

[return to 172.29.167.179]

2.1.4 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

Summary
This NVT summarizes technical information about the scanned host collected during the scan.

Vulnerability Detection Result
`traceroute:172.29.167.180,172.29.167.179`
`TCP ports:80,22`
`UDP ports:`

Log Method
Details: `Host Summary`
OID:1.3.6.1.4.1.25623.1.0.810003
Version used: `$Revision: 8287 $`

[return to 172.29.167.179]

2.1.5 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
`172.29.167.179|cpe:/a:gnu:bash:4.4.19`
`172.29.167.179|cpe:/a:gnu:gzip:1.2.4`
`172.29.167.179|cpe:/a:gnu:gzip:1.6`
`172.29.167.179|cpe:/a:isc:dhcp:4.3.5`
`172.29.167.179|cpe:/a:openbsd:openssh:7.6p1`
`172.29.167.179|cpe:/a:openssl:openssl:1.1.0g`
`172.29.167.179|cpe:/a:ruby-lang:ruby:2.5.1.p57:p57`
`172.29.167.179|cpe:/a:vmware:open-vm-tools:10.3.0.5330`

. . . continues on next page . . .

... continued from previous page ...

172.29.167.179	cpe:/o:canonical:ubuntu_linux:18.04:-:lts

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 12413 $

[return to 172.29.167.179]

2.1.6 Log general/tcp

Log (CVSS: 0.0)
NVT: Firewall Enabled

Summary
The remote host is behind a firewall
Description :
Based on the responses obtained by the TCP scanner, it was possible to determine that the remote host seems to be protected by a firewall.
Important: This plugin only works if OpenVAS TCP Scanner was used.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
None

Log Method
Details: Firewall Enabled
OID:1.3.6.1.4.1.25623.1.0.80059
Version used: $Revision: 7176 $

Log (CVSS: 0.0)
NVT: GNU Bash Version Detection (Linux)

Summary
Detects the installed version of GNU bash.
The script logs in via SSH, searches for the executable 'bash' and queries the found executables via the command line option '–version'

Vulnerability Detection Result
Detected GNU bash
Version: 4.4.19
Location: /bin/bash
CPE: cpe:/a:gnu:bash:4.4.19

... continues on next page ...

... continued from previous page ...

```
Concluded from version/product identification result:
GNU bash, version 4.4.19
```

Log Method
Details: GNU Bash Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.108258
Version used: $Revision: 12551 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.6
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.6
Concluded from version identification result:
gzip 1.6
Copyright (C) 2007, 2010, 2011 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.

Written by Jean-loup Gailly.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary
Detects the installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.2.4
```

... continues on next page ...

... continued from previous page ...

```
Location: /usr/lib/klibc/bin/gzip
CPE: cpe:/a:gnu:gzip:1.2.4
Concluded from version identification result:
gzip 1.2.4 (18 Aug 93)
usage: gzip [-cdfhlLnNtvV19] [-S suffix] [file ...]
 -c --stdout      write on standard output, keep original files unchanged
 -d --decompress  decompress
 -f --force       force overwrite of output file and compress links
 -h --help        give this help
 -L --license     display software license
 -n --no-name     do not save or restore the original name and time stamp
 -N --name        save or restore the original name and time stamp
 -q --quiet       suppress all warnings
 -S .suf  --suffix .suf     use suffix .suf on compressed files
 -t --test        test compressed file integrity
 -v --verbose     verbose mode
 -V --version     display version number
 file...          files to decompress. If none given, use standard input.
```

Log Method
Details: GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: ISC DHCP Client Version Detection

Summary
Detects the installed version of ISC DHCP Client.
The script logs in via ssh, searches for executable 'dhclient' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected ISC DHCP Client version: 4.3.5
Location: /sbin/dhclient
CPE: cpe:/a:isc:dhcp:4.3.5
Concluded from version identification result:
isc-dhclient-4.3.5
```

Log Method
Details: ISC DHCP Client Version Detection
OID:1.3.6.1.4.1.25623.1.0.900696
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detects the installed version of OpenSSL.
The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result
```
Detected OpenSSL
Version:  1.1.0g
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:1.1.0g
Concluded from version/product identification result:
OpenSSL 1.1.0g  2 Nov 2017
```

Log Method
Details: `OpenSSL Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: `$Revision: 11279 $`

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the references community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: Ubuntu 18.04 LTS
CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪1
```

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 12700 $

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary
Detects the installed version of Ruby.
The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
Detected Ruby version: 2.5.1.p57
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:2.5.1.p57:p57
Concluded from version identification result:
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]

Log Method
Details: Ruby Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: $Revision: 11279 $

Log (CVSS: 0.0)
NVT: SSH Authenticated Scan Info Consolidation

Summary
This script consolidates various technical information about authenticated scans via SSH.

Vulnerability Detection Result
Description (Knowledge base entry)
↪ Value/Content

↪ ---
Also use 'find' command to search for Applications enabled within 'Options for L
↪ocal Security Checks' (ssh/lsc/enable_find) : yes
Amount of timeouts the 'find' command has reached. (ssh/lsc/find_timeout)
↪ : None

... continues on next page ...

... continued from previous page ...

```
Clear received buffer before sending a command (ssh/force/clear_buffer)
↪                                                    : FALSE
Commands are send via an pseudoterminal/pty (ssh/force/pty)
↪                                                    : FALSE
Debugging enabled within 'Global variable settings' (global_settings/ssh/debug)
↪                                                    : FALSE
Descend directories on other filesystem enabled within 'Options for Local Securi
↪ty Checks' (ssh/lsc/descend_ofs)                    : yes
Don't prepend '/bin/sh -c' to used commands (ssh/force/nosh)
↪                                                    : FALSE
FreeBSD patchlevel (ssh/login/freebsdpatchlevel)
↪                                                    : Not applicable for target
FreeBSD release (ssh/login/freebsdrel)
↪                                                    : Not applicable for target
Login on a system with a restricted shell (ssh/restricted_shell)
↪                                                    : FALSE
Login on a system without common commands like 'cat' or 'find' (ssh/no_linux_she
↪ll)                                                 : FALSE
Login successful (login/SSH/success)
↪                                                    : TRUE
Mac OS X build (ssh/login/osx_build)
↪                                                    : Not applicable for target
Mac OS X release name (ssh/login/osx_name)
↪                                                    : Not applicable for target
Mac OS X version (ssh/login/osx_version)
↪                                                    : Not applicable for target
Misconfigured CISCO device. No autocommand should be configured for the scanning
↪ user. (ssh/cisco/broken_autocommand)               : FALSE
OpenBSD version (ssh/login/openbsdversion)
↪                                                    : Not applicable for target
Operating System Key used (ssh/login/release)
↪                                                    : UBUNTU18.04 LTS
Port used for authenciated scans (kb_ssh_transport())
↪                                                    : 22/tcp
Response to 'uname -a' command (ssh/login/uname)
↪                                                    : FALSE
Send an extra command (ssh/send_extra_cmd)
↪                                                    : FALSE
Solaris hardware type (ssh/login/solhardwaretype)
↪                                                    : Not applicable for target
Solaris version (ssh/login/solosversion)
↪                                                    : Not applicable for target
User used for authenciated scans (kb_ssh_login())
↪                                                    : vagrant
locate: Command available (ssh/locate/available)
↪                                                    : TRUE
```

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details: `SSH Authenticated Scan Info Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108162
Version used: `$Revision: 9954 $`

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
```
Here is the route from 172.29.167.180 to 172.29.167.179:
172.29.167.180
172.29.167.179
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 10411 $`

Log (CVSS: 0.0)
NVT: VMware Open Virtual Machine Tools Version Detection

Summary
This script finds the installed VMware Open Virtual Machine Tools version and saves the result in KB.

Vulnerability Detection Result
```
VMware Open Virtual Machine Tools  version 10.3.0.5330 build 8931395 running at
↪location /usr/bin/vmtoolsd was detected on the host
```

Log Method
Details: `VMware Open Virtual Machine Tools Version Detection`
OID:1.3.6.1.4.1.25623.1.0.801916
Version used: `$Revision: 11015 $`

[return to 172.29.167.179]

2.1.7 Log general/icmp

Log (CVSS: 0.0) NVT: Record route
Summary This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
`Here is the route recorded between 172.29.167.180 and 172.29.167.179 :`
`172.29.167.179.`
`172.29.167.179.`

Log Method Details: `Record route` OID:1.3.6.1.4.1.25623.1.0.12264 Version used: `$Revision: 10411 $`

[return to 172.29.167.179]

2.1.8 Log 22/tcp

Log (CVSS: 0.0) NVT: Check open ports
Summary This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result
`This port was detected as being open by a port scanner but is now closed.`
`This service might have been crashed by a port scanner or by a plugin`

Log Method Details: `Check open ports` OID:1.3.6.1.4.1.25623.1.0.10919 Version used: `$Revision: 5348 $`

Log (CVSS: 0.0) NVT: Determine OS and list of installed packages via SSH login
Summary This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.
. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
`We are able to login and detect that you are running Ubuntu 18.04 LTS`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details: `Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 12560 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 10922 $`

Log (CVSS: 0.0)
NVT: SSH Authorization Check

Summary
This script tries to login with provided credentials.
If the login was successful, it marks this port as available for any authenticated tests.

Vulnerability Detection Result
`It was possible to login using the provided SSH credentials. Hence authenticated`

... continues on next page ...

... continued from previous page ...

```
↪ checks are enabled.
```

Log Method
Details: SSH Authorization Check
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: $Revision: 10873 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-sha1
server_host_key_algorithms:
ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method
Details: SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 9609 $

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result
```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint:
ecdsa-sha2-nistp256: f0:32:b8:97:a8:41:86:e9:a5:62:f0:c0:20:b4:fa:32
ssh-ed25519: 94:8d:6f:a4:34:4a:23:26:f5:fa:1f:6b:27:d9:a5:d8
ssh-rsa: a5:66:fa:54:40:6c:d2:2f:b5:0e:fd:e0:85:7f:28:f8
```

Log Method
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 10929 $`

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary
This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result
```
Remote SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1
Remote SSH supported authentication: publickey
Remote SSH banner: (not available)
CPE: cpe:/a:openbsd:openssh:7.6p1
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method
Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 10902 $`

[return to 172.29.167.179]

2.1.9 False Positive general/tcp

False Positive (Overridden from Medium)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation could result in Denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive.

Solution
Solution type: VendorFix
Update to GZip version 1.3.13 or later.

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details: `GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: `$Revision: 12690 $`

References
```
CVE: CVE-2009-2624
BID:37888
Other:
  URL:http://secunia.com/advisories/38132
   URL:http://www.vupen.com/english/advisories/2010/0185
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
   URL:http://www.gzip.org/index-f.html#sources
   URL:http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b00747338
↪1dba5032f4dfc1744cf2
```

[return to 172.29.167.179]