Scan Report

February 2, 2026

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 "Immediate scan of IP 10.67.129.177". The scan started at Mon Feb 2 15:26:59 2026 UTC and ended at Mon Feb 2 15:46:13 2026 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

Result Overview

Host	High	Medium	Low	Log	False Positive
10.67.129.177	0	3	1	16	0
Total: 1	0	3	1	16	0

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 20 results selected by the filtering described above. Before filtering there were 20 results.

Results per Host

10.67.129.177

Host scan start	Mon Feb 2 15:27:21 2026 UTC
Host scan end	Mon Feb 2 15:46:13 2026 UTC

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

Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
`The following input fields where identified (URL:input name):`
`http://10.67.129.177/phpMyAdmin/:pma_password`

. . . continues on next page . . .

... continued from previous page ...

http://10.67.129.177/phpMyAdmin/?D=A:pma_password
http://10.67.129.177/v2/admin/login.html:pass

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: $Revision: 10726 $

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 5.0)
NVT: Enabled Directory Listing Detection

Summary
The script attempts to identify directories with an enabled directory listing.

Vulnerability Detection Result
The following directories with an enabled directory listing were identified:
http://10.67.129.177/phpMyAdmin/doc/html/_images
http://10.67.129.177/phpMyAdmin/doc/html/_sources
http://10.67.129.177/phpMyAdmin/doc/html/_static

... continues on next page ...

... continued from previous page ...

Please review the content manually.

Impact
Based on the information shown an attacker might be able to gather additional info about the structure of this application.

Solution
Solution type: Mitigation
If not needed disable the directory listing within the webservers config.

Affected Software/OS
Webservers with an enabled directory listing.

Vulnerability Detection Method
Check the detected directories if a directory listing is enabled.
Details: Enabled Directory Listing Detection
OID:1.3.6.1.4.1.25623.1.0.111074
Version used: $Revision: 5440 $

References
Other:
URL:https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing

[return to 10.67.129.177]

Medium general/tcp

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

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

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Solution type: VendorFix
Please see the referenced advisories for more information on obtaining and applying fixes.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

TCP/IP v4

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Details: `TCP Sequence Number Approximation Reset Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: `$Revision: 11066 $`

References
`CVE: CVE-2004-0230`
`BID:10183`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/15886`
`URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006`
`URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx`
`URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`

[return to 10.67.129.177]

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:
Packet 1: 369770284
Packet 2: 369771425
```

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

... continues on next page ...

... continued from previous page ...

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 the references for more information.

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: 14310 $`

References
```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 10.67.129.177]

Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache Web Server Detection

Summary
Detects the installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.

Vulnerability Detection Result
```
Detected Apache
Version:  2.4.41
Location: 80/tcp
CPE:      cpe:/a:apache:http_server:2.4.41
```

... continues on next page ...

... continued from previous page ...

```
Concluded from version/product identification result:
Server: Apache/2.4.41
```

Log Method
Details: Apache Web Server Detection
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: $Revision: 10290 $

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)
- 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 this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "10.67.129.177" 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 NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-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.
A possible recursion was detected during CGI scanning:
The service is using a relative URL in one or more HTML references where e.g. /f
↪ile1.html contains <a href="subdir/file2.html"> and a subsequent request for s
↪ubdir/file2.html is linking to subdir/file2.html. This would resolves to subdi
↪r/subdir/file2.html causing a recursion. To work around this counter-measures
↪have been enabled but the service should be fixed as well to not use such prob
↪lematic links. Below an excerpt of URLs is shown to help identify those issues
↪.
Syntax : URL (HTML link)
```

... continues on next page ...

... continued from previous page ...

```
http://10.67.129.177/phpMyAdmin/ (themes/dot.gif)
http://10.67.129.177/phpMyAdmin/?D=A (themes/dot.gif)
http://10.67.129.177/phpMyAdmin/doc/html/ (_sources/index.rst.txt)
http://10.67.129.177/phpMyAdmin/doc/html/ (_static/classic.css)
http://10.67.129.177/phpMyAdmin/doc/html/ (_static/doctools.js)
The following directories were used for CGI scanning:
http://10.67.129.177/
http://10.67.129.177/phpMyAdmin
http://10.67.129.177/phpMyAdmin/doc/html
http://10.67.129.177/phpMyAdmin/doc/html/_images
http://10.67.129.177/phpMyAdmin/doc/html/_sources
http://10.67.129.177/phpMyAdmin/doc/html/_static
http://10.67.129.177/v2/admin
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
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://10.67.129.177/assets/blogCarrer/css
http://10.67.129.177/assets/css
http://10.67.129.177/assets/css/bootstrap
http://10.67.129.177/assets/css/owl-carousel
http://10.67.129.177/assets/images
http://10.67.129.177/assets/img
http://10.67.129.177/assets/js
http://10.67.129.177/assets/js/bootstrap
http://10.67.129.177/assets/js/vendor
http://10.67.129.177/assets/js/vendor/owl-carousel
http://10.67.129.177/icons
http://10.67.129.177/js
http://10.67.129.177/phpMyAdmin/js
http://10.67.129.177/phpMyAdmin/js/dist
http://10.67.129.177/phpMyAdmin/js/dist/codemirror/addon/lint
http://10.67.129.177/phpMyAdmin/js/vendor
http://10.67.129.177/phpMyAdmin/js/vendor/bootstrap
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/hint
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/lint
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/runmode
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/lib
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/mode/sql
http://10.67.129.177/phpMyAdmin/js/vendor/jquery
http://10.67.129.177/phpMyAdmin/themes
http://10.67.129.177/phpMyAdmin/themes/pmahomme/css
http://10.67.129.177/phpMyAdmin/themes/pmahomme/img
```

... continues on next page ...

... continued from previous page ...

```
http://10.67.129.177/phpMyAdmin/themes/pmahomme/jquery
Directory index found at:
http://10.67.129.177/phpMyAdmin/doc/html/_images/
http://10.67.129.177/phpMyAdmin/doc/html/_static/
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://10.67.129.177/phpMyAdmin/doc/html/_images/ (C=S;O [A] C=N;O [D] C=M;O [A]
↪ C=D;O [A] )
http://10.67.129.177/phpMyAdmin/doc/html/_sources/ (C=S;O [A] C=N;O [D] C=M;O [A
↪] C=D;O [A] )
http://10.67.129.177/phpMyAdmin/doc/html/_static/ (C=S;O [A] C=N;O [D] C=M;O [A]
↪ C=D;O [A] )
http://10.67.129.177/phpMyAdmin/doc/html/search.html (check_keywords [yes] q []
↪area [default] )
http://10.67.129.177/phpMyAdmin/index.php (token [516551444f273a44235b286c6b7f4f
↪5d] pma_username [] table [] route [/] set_session [qqj3oq4sp954pnnlnnio0up8el
↪] lang [en] server [1] db [] pma_password [] )
http://10.67.129.177/phpMyAdmin/js/messages.php (l [en] lang [en] v [5.1.0] )
http://10.67.129.177/phpMyAdmin/url.php (url [https%3A%2F%2Fwww.phpmyadmin.net%2
↪F] )
http://10.67.129.177/v2/admin/logincheck.php (user [] ci_csrf_token [] pass [] )
http://10.67.129.177/v2/admin/register.html ()
http://10.67.129.177/v2/admin/track_orders (awb [] )
The following cgi scripts were excluded from CGI scanning because of the "Regex
↪pattern to exclude cgi scripts" setting of the NVT "Web mirroring" (OID: 1.3.6
↪.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
http://10.67.129.177/phpMyAdmin/js/dist/ajax.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/codemirror/addon/lint/sql-lint.js (v [5.
↪1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/common.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/config.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/console.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/cross_framing_protection.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/doclinks.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/drag_drop_import.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/error_report.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/functions.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/indexes.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/keyhandler.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/menu_resizer.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/navigation.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/page_settings.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/rte.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/dist/shortcuts_handler.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/bootstrap/bootstrap.bundle.min.js (v [
↪5.1.0] )
```

... continues on next page ...

... continued from previous page ...

```
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/hint/show-hint.css (v
↪ [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/hint/show-hint.js (v
↪[5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/hint/sql-hint.js (v [
↪5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/lint/lint.css (v [5.1
↪.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/lint/lint.js (v [5.1.
↪0] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/addon/runmode/runmode.js (v
↪ [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/lib/codemirror.css (v [5.1.
↪0] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/lib/codemirror.js (v [5.1.0
↪] )
http://10.67.129.177/phpMyAdmin/js/vendor/codemirror/mode/sql/sql.js (v [5.1.0]
↪)
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery-migrate.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery-ui-timepicker-addon.js (
↪v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery-ui.min.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery.ba-hashchange-2.0.js (v
↪[5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery.debounce-1.0.6.js (v [5.
↪1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery.event.drag-2.2.js (v [5.
↪1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery.min.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery.mousewheel.js (v [5.1.0]
↪ )
http://10.67.129.177/phpMyAdmin/js/vendor/jquery/jquery.validate.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/js.cookie.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/sprintf.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/js/vendor/tracekit.js (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/themes/pmahomme/css/printview.css (v [5.1.0] )
http://10.67.129.177/phpMyAdmin/themes/pmahomme/css/theme.css (server [1] nocach
↪e [3228293707ltr] v [5.1.0] )
```

Log Method
Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 13679 $`

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

Log (CVSS: 0.0)
NVT: Fingerprint web server with favicon.ico

Summary
The remote web server contains a graphic image that is prone to information disclosure.

Vulnerability Detection Result
```
The following apps/services were identified:
"phpmyadmin (4.6.x)" fingerprinted by the file: "http://10.67.129.177/phpMyAdmin
↪/favicon.ico"
```

Impact
The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

Solution
Solution type: Mitigation
Remove the 'favicon.ico' file or create a custom one for your site.

Log Method
Details: `Fingerprint web server with favicon.ico`
OID:1.3.6.1.4.1.25623.1.0.20108
Version used: `$Revision: 11730 $`

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result
```
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

... continues on next page ...

... continued from previous page ...

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
   URL:https://securityheaders.io/
```

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

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result

```
The remote web server type is :
Apache/2.4.41 (Ubuntu)
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
```

Solution
- Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 11585 $`

Log (CVSS: 0.0)
NVT: jQuery Detection

Summary
Detection of jQuery.
The script sends a connection request to the server and attempts to detect jQuery and to extract its version.

Vulnerability Detection Result

```
Detected jQuery
Version:  3.5.1
Location: /phpMyAdmin/js/vendor/jquery
CPE:      cpe:/a:jquery:jquery:3.5.1
Concluded from version/product identification result:
jQuery v3.5.1
Concluded from version/product identification location:
```

... continues on next page ...

... continued from previous page ...

/phpMyAdmin/js/vendor/jquery/jquery.min.js

Log Method
Details: jQuery Detection
OID:1.3.6.1.4.1.25623.1.0.141622
Version used: $Revision: 14001 $

References
Other:
URL:https://jquery.com/

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection

Summary
Detection of phpMyAdmin.
The script sends a connection request to the server and attempts to extract the version number from the reply.

Vulnerability Detection Result
Detected phpMyAdmin
Version: 5.1.0
Location: /phpMyAdmin
CPE: cpe:/a:phpmyadmin:phpmyadmin:5.1.0
Concluded from version/product identification result:
Version 5.1.0
Concluded from version/product identification location:
http://10.67.129.177/phpMyAdmin/README
Extra information:
- Protected by Username/Password

Log Method
Details: phpMyAdmin Detection
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: $Revision: 12754 $

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

... continues on next page ...

... continued from previous page ...

A web server is running on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

Summary
This plugin uses wapiti to find web security issues.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
See the preferences section for wapiti options.
Note that the scanner is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Note: The plugin needs the 'wapiti' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result
The wapiti report filename is empty. That could mean that a wrong version of wap
↪iti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapi
↪ti 1.x is not supported.
In short: Check the installation of wapiti and the scanner.

Log Method
Details: wapiti (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.80110
Version used: $Revision: 13985 $

[return to 10.67.129.177]

Log general/tcp

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 referenced community portal.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Best matching OS:
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
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_8.2p1 Ubuntu-4ubuntu0.
↪13
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.41 (Ubuntu)
OS: Debian GNU/Linux or Ubuntu
CPE: cpe:/o:debian:debian_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server default page on port 80/tcp: http://10.67.129.177/ind
↪ex.nginx-debian.html
```

Log Method

Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 14244 $

References

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

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 172.17.0.2 to 10.67.129.177:
172.17.0.2
10.67.129.177
```

Solution

Block unwanted packets from escaping your network.

Log Method

... continues on next page ...

... continued from previous page ...

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

[return to 10.67.129.177]

Log 22/tcp

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: 13541 $`

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,kex-s
↪trict-s-v00@openssh.com
server_host_key_algorithms:
rsa-sha2-512,rsa-sha2-256,ssh-rsa,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
```

... continues on next page ...

... continued from previous page ...

```
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: 13581 $

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:
1.99
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: b0:89:a6:43:7f:c3:83:04:da:cc:f5:ab:97:33:0d:e1
ssh-rsa: ea:14:05:89:0d:d6:5a:75:b0:e1:83:4d:aa:3d:df:fc
```

Log Method
Details: SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 13594 $

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.

... continues on next page ...

... continued from previous page ...

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 banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.13
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
CPE: cpe:/a:openbsd:openssh:8.2p1
Concluded from remote connection attempt with credentials:
Login:    OpenVAS-VT
Password: OpenVAS-VT
```

Log Method

Details: SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: 2019-03-22T07:02:59+0000

[return to 10.67.129.177]

Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

```
10.67.129.177|cpe:/a:apache:http_server:2.4.41
10.67.129.177|cpe:/a:jquery:jquery:3.5.1
10.67.129.177|cpe:/a:openbsd:openssh:8.2p1
10.67.129.177|cpe:/a:phpmyadmin:phpmyadmin:5.1.0
10.67.129.177|cpe:/o:canonical:ubuntu_linux
```

Log Method

Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 14324 $

References

```
Other:
  URL:http://cpe.mitre.org/
```

[return to 10.67.129.177]

This file was automatically generated.