Scan Report

August 1, 2024

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 ones.bookings.one". The scan started at Thu Aug 1 03:47:17 2024 UTC and ended at Thu Aug 1 04:35:17 2024 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
52.187.36.104 ones.bookings.one	0	0	1	12	0
Total: 1	0	0	1	12	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
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.
Issues with the threat level "Debug" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 13 results selected by the filtering described above. Before filtering there were 14 results.

2 Results per Host

2.1 52.187.36.104

Host scan start	Thu Aug 1 03:48:18 2024 UTC
Host scan end	Thu Aug 1 04:35:12 2024 UTC

Service (Port)	Threat Level
general/tcp	Low
general/CPE-T	Log
1221/tcp	Log
4024/tcp	Log
general/tcp	Log

2.1.1 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Quality of Detection (QoD): 80%
. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2996569550
Packet 2: 2996571219

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 the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2023-12-15T16:10:08Z

References
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 52.187.36.104]

2.1.2 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.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`52.187.36.104|cpe:/o:microsoft:windows`

Solution:

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2022-07-27T10:11:28Z`

References
`url: https://nvd.nist.gov/products/cpe`

[return to 52.187.36.104]

2.1.3 Log 1221/tcp

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The host does not return '404 Not Found' error codes when a non-existent file is ↪ requested and it wasn't possible to find a common error message interpreted a ↪s a 404. Some HTTP-related checks have been disabled.`

Solution:

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2023-07-07T05:05:26Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP

Summary
This script checks if the remote HTTP server is sending a HPKP, HSTS and/or Expect-CT header via plain HTTP.
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote HTTP server is sending HPKP, HSTS and/or Expect-CT headers via plain
↪HTTP.
HSTS-Header:
Strict-Transport-Security: max-age=31536000
```

Solution:
Solution type: Workaround
Configure the remote host to only send HPKP, HSTS and Expect-CT headers via HTTPS. Sending those headers via plain HTTP doesn't comply with the referenced RFCs.

Log Method
Details: `SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP`
OID:1.3.6.1.4.1.25623.1.0.108248
Version used: `2023-07-25T05:05:58Z`

... continues on next page ...

... continued from previous page ...

References
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
url: https://owasp.org/www-project-secure-headers/#expect-ct
url: https://tools.ietf.org/html/rfc6797
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: http://httpwg.org/http-extensions/expect-ct.html#http-request-type

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

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: Microsoft-HTTPAPI/2.0

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

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

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

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Header Name             | Header Value
-----------------------------------
X-Content-Type-Options | nosniff
X-Frame-Options        | DENY
X-XSS-Protection       | 1
Missing Headers                   | More Information
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner                  | Enumeration technique
-------------------------------------------------------------------------------
↪----------------
Server: Microsoft-HTTPAPI/2.0 | Invalid HTTP 00.5 GET request (non-existent HTTP
↪ version) to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2022-06-28T10:11:01Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
A web server is running on this port

... continues on next page ...

... continued from previous page ...

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
The script consolidates and reports various information for web application (formerly called '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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The Hostname/IP "ones.bookings.one" 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; OpenVAS-VT 23.0.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
```

... continues on next page ...

... continued from previous page ...

```
http://ones.bookings.one:1221/
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
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-07-03T06:48:05Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

[return to 52.187.36.104]

2.1.4 Log 4024/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Nmap service detection (unknown) result for this port: tnp1-port
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 4024 52.187.36.104' and submit a possible collected
↪ fingerprint to the nmap database.
```

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108441
Version used: 2023-06-22T10:34:15Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

[return to 52.187.36.104]

2.1.5 Log general/tcp

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Hostname determination for IP 52.187.36.104:
Hostname|Source
ones.bookings.one|Forward-DNS

Solution:

Log Method
Details: Hostname Determination Reporting
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: 2022-07-27T10:11:28Z

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

Summary
This script consolidates the OS information detected by several VTs 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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Best matching OS:
OS:           Microsoft Windows
CPE:          cpe:/o:microsoft:windows
Found by VT:  1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server banner on port 1221/tcp: Server: Microsoft-HTTPAPI/2.
↪0
Setting key "Host/runs_windows" based on this information
```

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2024-07-30T05:05:46Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Network route from scanner (172.20.0.7) to target (52.187.36.104):
172.20.0.7
52.187.36.104
Network distance between scanner and target: 2
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: Traceroute

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.51662 Version used: 2022-10-17T11:13:19Z

[return to 52.187.36.104]
