

# Scan Report

April 18, 2018

## Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “America/Belem”, which is abbreviated “-03”. The task was “Alvo Paraiso”. The scan started at Wed Apr 18 11:09:05 2018 -03 and ended at Wed Apr 18 11:16:35 2018 -03. 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	200.239.72.19 . . . . .	2
2.1.1	Log general/HOST-T . . . . .	2
2.1.2	Log 22/tcp . . . . .	3
2.1.3	Log 21/tcp . . . . .	5
2.1.4	Log general/tcp . . . . .	6
2.1.5	Log 80/tcp . . . . .	8
2.1.6	Log general/CPE-T . . . . .	11
2.1.7	Log general/icmp . . . . .	11

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">200.239.72.19</a> <a href="#">host-200-239-19.ufpa.br</a>	0	0	0	17	0
Total: 1	0	0	0	17	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found.

It only lists hosts that produced issues.

Issues with the threat level “Debug” are not shown.

Issues with the threat level “False Positive” are not shown.

This report contains all 17 results selected by the filtering described above. Before filtering there were 26 results.

## 2 Results per Host

### 2.1 200.239.72.19

Host scan start Wed Apr 18 11:09:13 2018 -03

Host scan end Wed Apr 18 11:16:35 2018 -03

Service (Port)	Threat Level
<a href="#">general/HOST-T</a>	Log
<a href="#">22/tcp</a>	Log
<a href="#">21/tcp</a>	Log
<a href="#">general/tcp</a>	Log
<a href="#">80/tcp</a>	Log
<a href="#">general/CPE-T</a>	Log
<a href="#">general/icmp</a>	Log

#### 2.1.1 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

... continues on next page ...

...continued from previous page ...
<pre>tracert:10.15.10.20,10.200.3.4,200.239.72.19 TCP ports:80,21,22 UDP ports:</pre>
<b>Log Method</b> Details:Host Summary OID:1.3.6.1.4.1.25623.1.0.810003 Version used: \$Revision: 8287 \$

[\[ return to 200.239.72.19 \]](#)

### 2.1.2 Log 22/tcp

Log (CVSS: 0.0) NVT: SSH Protocol Versions Supported
<b>Summary</b> 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
<b>Vulnerability Detection Result</b> The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0 SSHv2 Fingerprint: ecdsa-sha2-nistp256: 68:d0:25:f3:55:ce:a4:02:26:ee:b5:29:c5:36:06:ab ssh-rsa: 63:f6:f3:13:73:9c:a3:72:18:85:94:63:7b:d3:4c:1a
<b>Log Method</b> Details:SSH Protocol Versions Supported OID:1.3.6.1.4.1.25623.1.0.100259 Version used: \$Revision: 4484 \$

Log (CVSS: 0.0) NVT: SSH Server type and version
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Remote SSH server version: SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u3 ...continues on next page ...

...continued from previous page ...
Remote SSH supported authentication: password,publickey Remote SSH banner: (not available) CPE: cpe:/a:openbsd:openssh:7.4p1 Concluded from remote connection attempt with credentials: Login: VulnScan Password: VulnScan
<b>Log Method</b> Details:SSH Server type and version OID:1.3.6.1.4.1.25623.1.0.10267 Version used: \$Revision: 7902 \$

Log (CVSS: 0.0) NVT: Services
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> An ssh server is running on this port
<b>Log Method</b> Details:Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 8188 \$

Log (CVSS: 0.0) NVT: SSH Protocol Algorithms Supported
<b>Summary</b> This script detects which algorithms and languages are supported by the remote SSH Service
<b>Vulnerability Detection Result</b> The following options are supported by the remote ssh service: kex_algorithms: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1 server_host_key_algorithms: ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256 encryption_algorithms_client_to_server: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com ...continues on next page ...

...continued from previous page ...

```

↪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: 7000 \$

[\[ return to 200.239.72.19 \]](#)**2.1.3 Log 21/tcp**

Log (CVSS: 0.0)

NVT: FTP Banner Detection

**Summary**

This Plugin detects the FTP Server Banner and the Banner of the 'HELP' command.

**Vulnerability Detection Result**

Remote FTP server banner :

220 (vsFTPd 3.0.3)

**Log Method**

Details:FTP Banner Detection

OID:1.3.6.1.4.1.25623.1.0.10092

Version used: \$Revision: 4780 \$

Log (CVSS: 0.0)

NVT: Services

**Summary**

...continues on next page ...

...continued from previous page ...
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.
<b>Vulnerability Detection Result</b> An FTP server is running on this port. Here is its banner : 220 (vsFTPd 3.0.3)
<b>Log Method</b> Details:Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 8188 \$

Log (CVSS: 0.0) NVT: vsFTPd FTP Server Detection
<b>Summary</b> The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.
<b>Vulnerability Detection Result</b> Detected vsFTPd Version: 3.0.3 Location: 21/tcp CPE: cpe:/a:beasts:vsftpd:3.0.3 Concluded from version/product identification result: 220 (vsFTPd 3.0.3)
<b>Log Method</b> Details:vsFTPd FTP Server Detection OID:1.3.6.1.4.1.25623.1.0.111050 Version used: \$Revision: 4777 \$

[\[ return to 200.239.72.19 \]](#)

#### 2.1.4 Log general/tcp

Log (CVSS: 0.0) NVT: OS Detection Consolidation and Reporting
<b>Summary</b> This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
... continues on next page ...

...continued from previous page ...

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 [openvas-plugins@wald.intevation.org](mailto:openvas-plugins@wald.intevation.org).

### Vulnerability Detection Result

Best matching OS:

OS: Debian GNU/Linux 9

Version: 9

CPE: cpe:/o:debian:debian\_linux:9

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\_7.4p1 Debian-10+deb9u3

Setting key "Host/runs\_unixoid" based on this information

Other OS detections (in order of reliability):

OS: Linux/Unix

CPE: cpe:/o:linux:kernel

Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)

Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 3.0.3)

OS: Debian GNU/Linux

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 banner on port 80/tcp: Server: Apache/2.4.25 (Debian)

OS: Debian GNU/Linux

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: <title>Apache2 Debian De  
↪fault Page

### Log Method

Details: OS Detection Consolidation and Reporting

OID: 1.3.6.1.4.1.25623.1.0.105937

Version used: \$Revision: 9462 \$

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 10.15.10.20 to 200.239.72.19:

10.15.10.20

10.200.3.4

... continues on next page ...

...continued from previous page ...
200.239.72.19
<b>Solution</b> Block unwanted packets from escaping your network.
<b>Log Method</b> Details:Traceroute OID:1.3.6.1.4.1.25623.1.0.51662 Version used: \$Revision: 8528 \$

[\[ return to 200.239.72.19 \]](#)

### 2.1.5 Log 80/tcp

Log (CVSS: 0.0) NVT: HTTP Server type and version
<b>Summary</b> This detects the HTTP Server's type and version.
<b>Vulnerability Detection Result</b> The remote web server type is : Apache/2.4.25 (Debian) Solution : You can set the directive "ServerTokens Prod" to limit the information emanating from the server in its response headers.
<b>Solution</b>
<b>Log Method</b> Details:HTTP Server type and version OID:1.3.6.1.4.1.25623.1.0.10107 Version used: \$Revision: 8370 \$

Log (CVSS: 0.0) NVT: Services
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> A web server is running on this port
...continues on next page ...



...continued from previous page ...

**Log Method**

Details:Services

OID:1.3.6.1.4.1.25623.1.0.10330

Version used: \$Revision: 8188 \$

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)

- 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 [openvas-plugins@wald.intevation.org](mailto:openvas-plugins@wald.intevation.org)

**Vulnerability Detection Result**

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the 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.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. 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://host-200-239-19.ufpa.br/>

<http://host-200-239-19.ufpa.br/cgi-bin>

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from CGI scanning because of the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288):

<http://host-200-239-19.ufpa.br/icons>

**Log Method**

Details:CGI Scanning Consolidation

OID:1.3.6.1.4.1.25623.1.0.111038

...continues on next page ...

...continued from previous page ...

Version used: \$Revision: 9467 \$

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: 8141 \$

**References**

Other:

URL:[https://www.owasp.org/index.php/OWASP\\_Secure-Headers\\_Project](https://www.owasp.org/index.php/OWASP_Secure-Headers_Project)URL:[https://www.owasp.org/index.php/OWASP\\_Secure-Headers\\_Project#tab=Headers](https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#tab=Headers)URL:<https://securityheaders.io/>

Log (CVSS: 0.0)

NVT: Apache Web Server Version Detection

**Summary**

Detection of 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: 2.4.25

Location: 80/tcp

CPE: cpe:/a:apache:http\_server:2.4.25

Concluded from version/product identification result:

Server: Apache/2.4.25

...continues on next page ...

...continued from previous page ...

**Log Method**

Details:Apache Web Server Version Detection

OID:1.3.6.1.4.1.25623.1.0.900498

Version used: \$Revision: 8140 \$

[\[ return to 200.239.72.19 \]](#)**2.1.6 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**

200.239.72.19|cpe:/a:apache:http\_server:2.4.25

200.239.72.19|cpe:/a:beasts:vsftpd:3.0.3

200.239.72.19|cpe:/a:openbsd:openssh:7.4p1

200.239.72.19|cpe:/o:debian:debian\_linux:9

**Log Method**

Details:CPE Inventory

OID:1.3.6.1.4.1.25623.1.0.810002

Version used: \$Revision: 8140 \$

[\[ return to 200.239.72.19 \]](#)**2.1.7 Log general/icmp**

Log (CVSS: 0.0)

NVT: ICMP Timestamp Detection

**Summary**

The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

**Vulnerability Detection Result**

... continues on next page ...

...continued from previous page ...
Vulnerability was detected according to the Vulnerability Detection Method.
<b>Log Method</b> Details:ICMP Timestamp Detection OID:1.3.6.1.4.1.25623.1.0.103190 Version used: \$Revision: 7559 \$
<b>References</b> CVE: CVE-1999-0524 Other: URL: <a href="http://www.ietf.org/rfc/rfc0792.txt">http://www.ietf.org/rfc/rfc0792.txt</a>

[ [return to 200.239.72.19](#) ]

---

This file was automatically generated.