# Scan Report

May 1, 2023

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "America/Sao$_Paulo$", $which is abbreviated$ "−03". $The task was$ "$Immediate scan of IP$ 10.0.0.22". $The scan started at Mon$ 33 : 522023−03 $and ended at Mon May$ 121 : 08 : 232023−03. $The report first summarises the results found. Then, for each host, the$

## Contents

**1 Result Overview** **2**

**2 Results per Host** **2**

2.1 10.0.0.22 . . . . . 2

2.1.1 Medium 8080/tcp . . . . . 2

2.1.2 Medium 22/tcp . . . . . 4

2.1.3 Medium 80/tcp . . . . . 7

2.1.4 Low general/tcp . . . . . 8

2.1.5 Low general/icmp . . . . . 9

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 10.0.0.22 | 0 | 5 | 2 | 0 | 0 |
| Total: 1 | 0 | 5 | 2 | 0 | 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 "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 7 results selected by the filtering described above. Before filtering there were 198 results.

# 2 Results per Host

## 2.1 10.0.0.22

| | |
|---|---|
| Host scan start | Mon May 1 20:34:30 2023 -03 |
| Host scan end | Mon May 1 21:08:16 2023 -03 |

| Service (Port) | Threat Level |
|---|---|
| 8080/tcp | Medium |
| 22/tcp | Medium |
| 80/tcp | Medium |
| general/tcp | Low |
| general/icmp | Low |

### 2.1.1 Medium 8080/tcp

Medium (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files

**Product detection result**
`cpe:/a:apache:tomcat:7.0.76`
`Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10`
`↪7652)`

. . . continues on next page . . .

... continued from previous page ...

**Summary**
The Apache Tomcat servlet/JSP container has default files installed.

**Vulnerability Detection Result**
`The following default files were found :`
`http://10.0.0.22:8080/examples/servlets/index.html`
`http://10.0.0.22:8080/examples/jsp/snp/snoop.jsp`
`http://10.0.0.22:8080/examples/jsp/index.html`

**Impact**
These files should be removed as they may help an attacker to guess the exact version of the Apache Tomcat which is running on this host and may provide other useful information.

**Solution:**
**Solution type:** Mitigation
Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.

**Vulnerability Insight**
Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.

**Vulnerability Detection Method**
Details: `Apache Tomcat servlet/JSP container default files`
OID:1.3.6.1.4.1.25623.1.0.12085
Version used: `2020-05-08T08:34:44Z`

**Product Detection Result**
Product: `cpe:/a:apache:tomcat:7.0.76`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

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 URLs requires Basic Authentication (URL:realm name):`
`http://10.0.0.22:8080/host-manager/html:"Tomcat Host Manager Application"`
`http://10.0.0.22:8080/manager/html:"Tomcat Manager Application"`
`http://10.0.0.22:8080/manager/status:"Tomcat Manager Application"`

... continues on next page ...

... continued from previous page ...

**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: `2020-08-24T15:18:35Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 10.0.0.22 ]

### 2.1.2 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Vulnerability Detection Result**
`The remote SSH server supports the following weak KEX algorithm(s):`
`KEX algorithm | Reason`

... continues on next page ...

... continued from previous page ...

```
------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2021-11-24T06:31:19Z`

**References**

```
url: https://weakdh.org/sysadmin.html
url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html
url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.sectio
↪n.5
url: https://datatracker.ietf.org/doc/html/rfc6194
```

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- none algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2021-09-20T08:25:27Z`

**References**
`url: https://tools.ietf.org/html/rfc4253#section-6.3`
`url: https://www.kb.cert.org/vuls/id/958563`

[ return to 10.0.0.22 ]

### 2.1.3 Medium 80/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

**Summary**
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

**Vulnerability Detection Result**
`The web server has the following HTTP methods enabled: TRACE`

**Impact**
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution:**
**Solution type:** Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

**Affected Software/OS**
Web servers with enabled TRACE and/or TRACK methods.

**Vulnerability Insight**
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

**Vulnerability Detection Method**
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2022-05-12T09:32:01Z`

**References**
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2012-2223
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

[ return to 10.0.0.22 ]

### 2.1.4 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/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1141428440
Packet 2: 1141429515
```

**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.

... continues on next page ...

... continued from previous page ...

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`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

**References**
`url: http://www.ietf.org/rfc/rfc1323.txt`
`url: http://www.ietf.org/rfc/rfc7323.txt`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

[ return to 10.0.0.22 ]

### 2.1.5 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

**Summary**
The remote host responded to an ICMP timestamp request.

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

**Solution:**
**Solution type:** Mitigation
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)

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
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 Method**
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

**References**
`cve: CVE-1999-0524`
`url: http://www.ietf.org/rfc/rfc0792.txt`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[ return to 10.0.0.22 ]