Scan Report

April 30, 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 10.0.2.7". The scan started at Tue Apr 30 02:09:17 2024 UTC and ended at Tue Apr 30 02:24:18 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
10.0.2.7	1	3	3	0	0
Total: 1	1	3	3	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 50 are shown.

This report contains all 7 results selected by the filtering described above. Before filtering there were 183 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.2.7	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 10.0.2.7

Host scan start	Tue Apr 30 02:09:32 2024 UTC
Host scan end	Tue Apr 30 02:24:11 2024 UTC

Service (Port)	Threat Level
8009/tcp	High
8080/tcp	Medium
22/tcp	Medium
general/icmp	Low
22/tcp	Low
general/tcp	Low

2.1.1 High 8009/tcp

High (CVSS: 9.8)

NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

Summary
Apache Tomcat is prone to a remote code execution vulnerability (dubbed 'Ghostcat') in the AJP connector.

Quality of Detection: 99

Vulnerability Detection Result

```
It was possible to read the file "/WEB-INF/web.xml" through the AJP connector.
Result:
AB w\x0004 Ã\x0088 \x0003200  \x0003Â \x0007 =JSESSIONID=44A98F4E76678BBA46A069A
↪B344B8045; Path=/; HttpOnly Â \x0001 \x001Ctext/html;charset=ISO-8859-1 Â \x00
↪03 \x00041227 AB\x0004Ã\x008F\x0003\x0004Ã\x008B<?xml version="1.0" encoding="
↪UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">
  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>
</web-app>
 AB \x0002\x0005\x0001
```

Solution:
Solution type: VendorFix

. . . continues on next page . . .

... continued from previous page ...

Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on fixed versions.

Affected Software/OS
Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled.
Other products like JBoss or Wildfly which are using Tomcat might be affected as well.

Vulnerability Insight
Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.

Vulnerability Detection Method
Sends a crafted AJP request and checks the response.
Details: `Apache Tomcat AJP RCE Vulnerability (Ghostcat)`
OID:1.3.6.1.4.1.25623.1.0.143545
Version used: `2023-07-06T05:05:36Z`

References
`cve: CVE-2020-1938`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1`
`↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E`
`url: https://www.chaitin.cn/en/ghostcat`
`url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487`
`url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi`
`url: https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances`
`↪-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/`
`url: https://tomcat.apache.org/tomcat-7.0-doc/changelog.html`
`url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html`
`url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html`
`cert-bund: WID-SEC-2023-2480`
`cert-bund: CB-K20/0711`
`cert-bund: CB-K20/0705`
`cert-bund: CB-K20/0693`
`cert-bund: CB-K20/0555`
`cert-bund: CB-K20/0543`
`cert-bund: CB-K20/0154`
`dfn-cert: DFN-CERT-2021-1736`
`dfn-cert: DFN-CERT-2020-1508`
`dfn-cert: DFN-CERT-2020-1413`
`dfn-cert: DFN-CERT-2020-1276`
`dfn-cert: DFN-CERT-2020-1134`
`dfn-cert: DFN-CERT-2020-0850`
`dfn-cert: DFN-CERT-2020-0835`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0821
dfn-cert: DFN-CERT-2020-0569
dfn-cert: DFN-CERT-2020-0557
dfn-cert: DFN-CERT-2020-0501
dfn-cert: DFN-CERT-2020-0381

[return to 10.0.2.7]

2.1.2 Medium 8080/tcp

Medium (CVSS: 6.8)

NVT: Apache Tomcat servlet/JSP container default files

Product detection result
cpe:/a:apache:tomcat:9.0.7
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

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

Quality of Detection: 99

Vulnerability Detection Result
The following default files were found :
http://10.0.2.7:8080/examples/servlets/index.html
http://10.0.2.7:8080/examples/jsp/snp/snoop.jsp
http://10.0.2.7:8080/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

... continues on next page ...

... continued from previous page ...

Details: Apache Tomcat servlet/JSP container default files
OID:1.3.6.1.4.1.25623.1.0.12085
Version used: 2023-08-01T13:29:10Z

Product Detection Result
Product: cpe:/a:apache:tomcat:9.0.7
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.

Quality of Detection: 80

Vulnerability Detection Result
The following URLs requires Basic Authentication (URL:realm name):
http://10.0.2.7:8080/host-manager/html:"Tomcat Host Manager Application"
http://10.0.2.7:8080/manager/html:"Tomcat Manager Application"
http://10.0.2.7:8080/manager/status:"Tomcat Manager Application"

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)

... continues on next page ...

... continued from previous page ...

- 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: 2023-09-07T05:05:21Z

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 10.0.2.7]

2.1.3 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)

Product detection result
cpe:/a:openbsd:openssh:7.2p2
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Quality of Detection: 50

Vulnerability Detection Result
Installed version: 7.2p2
Fixed version: None
Installation
path / port: 22/tcp

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
All currently OpenSSH versions are known to be affected.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)`
OID:1.3.6.1.4.1.25623.1.0.117777
Version used: `2022-11-24T10:18:54Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.2p2`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
`cve: CVE-2016-20012`
`url: https://github.com/openssh/openssh-portable/pull/270`
`url: https://rushter.com/blog/public-ssh-keys/`
`url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak`
`cert-bund: CB-K21/0979`

[return to 10.0.2.7]

2.1.4 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

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

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

... continues on next page ...

... continued from previous page ...

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)

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.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.0.2.7]

2.1.5 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

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

Quality of Detection: 80

Vulnerability Detection Result
`The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):`

... continues on next page ...

... continued from previous page ...

```
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

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

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 10.0.2.7]

2.1.6 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: 80

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: 216072
```

... continues on next page ...

... continued from previous page ...

Packet 2: 216337

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 10.0.2.7]