Scan Report

December 29, 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 "Metas3". The scan started at Sun Dec 29 05:14:13 2024 UTC and ended at Sun Dec 29 05:40:17 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.5 METASPLOITABLE	1	2	1	0	0
Total: 1	1	2	1	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 4 results selected by the filtering described above. Before filtering there were 133 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.2.5 - METASPLOITABLE	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 10.0.2.5

Host scan start	Sun Dec 29 05:14:43 2024 UTC
Host scan end	Sun Dec 29 05:40:11 2024 UTC

Service (Port)	Threat Level
80/tcp	High
80/tcp	Medium
8180/tcp	Medium
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)

NVT: TWiki XSS and Command Execution Vulnerabilities

Summary
TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.2.4`

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution:
Solution type: VendorFix
Upgrade to version 4.2.4 or later.

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to:
- %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: `TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `2024-03-01T14:37:10Z`

References
`cve: CVE-2008-5304`
`cve: CVE-2008-5305`
`url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304`
`url: http://www.securityfocus.com/bid/32668`
`url: http://www.securityfocus.com/bid/32669`
`url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305`

[return to 10.0.2.5]

2.1.2 Medium 80/tcp

Medium (CVSS: 6.0)

NVT: TWiki CSRF Vulnerability

Summary
TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.3.1`

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution:
Solution type: VendorFix
Upgrade to version 4.3.1 or later.

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details: `TWiki CSRF Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: `2024-06-28T05:05:33Z`

References
`cve: CVE-2009-1339`
`url: http://secunia.com/advisories/34880`
`url: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258`
`url: http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff`
`↪-cve-2009-1339.txt`

[return to 10.0.2.5]

2.1.3 Medium 8180/tcp

Medium (CVSS: 4.3)

NVT: Apache Tomcat cal2.jsp Cross Site Scripting Vulnerability

Product detection result
cpe:/a:apache:tomcat:5.5.25
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
Vulnerable URL: http://10.0.2.5:8180/jsp-examples/cal/cal2.jsp?time=%74%65%73%74
↪%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%22%61%74%74%61%63%6B%22%29%3B%3C%2F
↪%73%63%72%69%70%74%3E

Impact
Successful exploitation will allow remote attackers to inject arbitrary HTML codes in the context of the affected web application.

Solution:
Solution type: VendorFix
Update your Apache Tomcat to a non-affected version.

Affected Software/OS
Apache Tomcat version 4.1.0 to 4.1.39, 5.0.0 to 5.0.28, 5.5.0 to 5.5.27 and 6.0.0 to 6.0.18

Vulnerability Insight
The issue is due to input validation error in time parameter in 'jsp/cal/cal2.jsp' file in calendar application.

Vulnerability Detection Method
Details: Apache Tomcat cal2.jsp Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800372
Version used: 2023-07-27T05:05:08Z

Product Detection Result
Product: cpe:/a:apache:tomcat:5.5.25
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

. . . continues on next page . . .

... continued from previous page ...

References

```
cve: CVE-2009-0781
url: http://www.packetstormsecurity.org/0903-exploits/CVE-2009-0781.txt
url: http://www.securityfocus.com/archive/1/archive/1/501538/100/0/threaded
url: http://tomcat.apache.org/security-6.html
url: http://tomcat.apache.org/security-5.html
url: http://tomcat.apache.org/security-4.html
dfn-cert: DFN-CERT-2012-1832
dfn-cert: DFN-CERT-2011-0465
dfn-cert: DFN-CERT-2010-1607
dfn-cert: DFN-CERT-2010-0986
dfn-cert: DFN-CERT-2010-0690
```

[return to 10.0.2.5]

2.1.4 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection (QoD): 80%

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: 612512
Packet 2: 612621
```

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.

... continues on next page ...

... continued from previous page ...

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 10.0.2.5]