Scan Report

June 17, 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 "scanning kali2". The scan started at Mon Jun 17 00:02:56 2024 UTC and ended at Mon Jun 17 00:02:57 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
127.0.0.1 localhost	3	2	0	0	0
Total: 1	3	2	0	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 5 results selected by the filtering described above. Before filtering there were 5 results.

2 Results per Host

2.1 127.0.0.1

Host scan start	Mon Jun 17 00:02:56 2024 UTC
Host scan end	Mon Jun 17 00:02:57 2024 UTC

Service (Port)	Threat Level
N/A	High
N/A	Medium

2.1.1 High

High (CVSS: 8.1)
NVT: CVE-2015-8960

Product detection result
`cpe:/a:ietf:transport_layer_security:1.2`
`Detected by CVE-2015-8960 (OID: CVE-2015-8960)`

Quality of Detection: 75

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
The host carries the product: cpe:/a:ietf:transport_layer_security:1.2
It is vulnerable according to: CVE-2015-8960.
The product was found at: 5432/tcp.
The TLS protocol 1.2 and earlier supports the rsa_fixed_dh, dss_fixed_dh, rsa_fi
↪xed_ecdh, and ecdsa_fixed_ecdh values for ClientCertificateType but does not d
↪irectly document the ability to compute the master secret in certain situation
↪s with a client secret key and server public key but not a server secret key,
↪which makes it easier for man-in-the-middle attackers to spoof TLS servers by
↪leveraging knowledge of the secret key for an arbitrary installed client X.509
↪ certificate, aka the "Key Compromise Impersonation (KCI)" issue.

Vulnerability Detection Method
Details: CVE-2015-8960
OID:CVE-2015-8960
Version used: 2023-01-30T17:33:00Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security:1.2
Method: CVE-2015-8960
OID: CVE-2015-8960)

High (CVSS: 7.5)
NVT: CVE-1999-1029

Product detection result
cpe:/a:ssh:ssh2:2.0
Detected by CVE-1999-1029 (OID: CVE-1999-1029)

Quality of Detection: 75

Vulnerability Detection Result
The host carries the product: cpe:/a:ssh:ssh2:2.0
It is vulnerable according to: CVE-1999-1029.
The product was found at: 22/tcp.
SSH server (sshd2) before 2.0.12 does not properly record login attempts if the
↪connection is closed before the maximum number of tries, allowing a remote att
↪acker to guess the password without showing up in the audit logs.

Vulnerability Detection Method
Details: CVE-1999-1029
OID:CVE-1999-1029
Version used: 2017-12-19T02:29:00Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:ssh:ssh2:2.0
Method: CVE-1999-1029
OID: CVE-1999-1029)

High (CVSS: 7.2)
NVT: CVE-2002-1715

Product detection result
cpe:/a:ssh:ssh2:2.0
Detected by CVE-2002-1715 (OID: CVE-2002-1715)

Quality of Detection: 75

Vulnerability Detection Result
The host carries the product: cpe:/a:ssh:ssh2:2.0
It is vulnerable according to: CVE-2002-1715.
The product was found at: 22/tcp.
SSH 1 through 3, and possibly other versions, allows local users to bypass restr
↪icted shells such as rbash or rksh by uploading a script to a world-writeable
↪directory, then executing that script to gain normal shell access.

Vulnerability Detection Method
Details: CVE-2002-1715
OID:CVE-2002-1715
Version used: 2017-07-11T01:29:00Z

Product Detection Result
Product: cpe:/a:ssh:ssh2:2.0
Method: CVE-2002-1715
OID: CVE-2002-1715)

[return to 127.0.0.1]

2.1.2 Medium

Medium (CVSS: 5.1)
NVT: CVE-2000-0217

Product detection result
cpe:/a:ssh:ssh2:2.0
Detected by CVE-2000-0217 (OID: CVE-2000-0217)

... continues on next page ...

... continued from previous page ...

Quality of Detection: 75

Vulnerability Detection Result
The host carries the product: cpe:/a:ssh:ssh2:2.0
It is vulnerable according to: CVE-2000-0217.
The product was found at: 22/tcp.
The default configuration of SSH allows X forwarding, which could allow a remote attacker to control a client's X sessions via a malicious xauth program.

Vulnerability Detection Method
Details: CVE-2000-0217
OID:CVE-2000-0217
Version used: 2008-09-10T19:03:00Z

Product Detection Result
Product: cpe:/a:ssh:ssh2:2.0
Method: CVE-2000-0217
OID: CVE-2000-0217)

Medium (CVSS: 5)
NVT: CVE-1999-1231

Product detection result
cpe:/a:ssh:ssh2:2.0
Detected by CVE-1999-1231 (OID: CVE-1999-1231)

Quality of Detection: 75

Vulnerability Detection Result
The host carries the product: cpe:/a:ssh:ssh2:2.0
It is vulnerable according to: CVE-1999-1231.
The product was found at: 22/tcp.
ssh 2.0.12, and possibly other versions, allows valid user names to attempt to enter the correct password multiple times, but only prompts an invalid user name for a password once, which allows remote attackers to determine user account names on the server.

Vulnerability Detection Method
Details: CVE-1999-1231
OID:CVE-1999-1231
Version used: 2017-12-19T02:29:00Z

Product Detection Result
Product: cpe:/a:ssh:ssh2:2.0

... continues on next page ...

... continued from previous page ...

Method: CVE-1999-1231
OID: CVE-1999-1231)

[return to 127.0.0.1]
