Scan Report

October 16, 2025

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 "Cloud Vista Security Assessment v2". The scan started at Thu Oct 16 05:50:37 2025 UTC and ended at Thu Oct 16 06:30:55 2025 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
20.44.214.63 livedemo.cloud-vista.co	0	6	1	0	0
Total: 1	0	6	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 7 results selected by the filtering described above. Before filtering there were 73 results.

2 Results per Host

2.1 20.44.214.63

Host scan start	Thu Oct 16 05:51:11 2025 UTC
Host scan end	Thu Oct 16 06:30:52 2025 UTC

Service (Port)	Threat Level
5044/tcp	Medium
8444/tcp	Medium
514/tcp	Medium
general/tcp	Low

2.1.1 Medium 5044/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25`

... continues on next page ...

... continued from previous page ...

↪623.1.0.103692)

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost
Certificate details:
fingerprint (SHA-1)                | 744EC6629479417277FAC6065186C28C136A921F
fingerprint (SHA-256)              | 0315B850391B42C84B8E8039DC1E944D262095C9567E84
↪2B8F17205B69F4A33D
issued by                          | CN=localhost
public key algorithm               | RSA
public key size (bits)             | 2048
serial                             | 00A67EF443813499F3
signature algorithm                | sha256WithRSAEncryption
subject                            | CN=localhost
subject alternative names (SAN)    | None
valid from                         | 2021-09-23 11:23:43 UTC
valid until                        | 2021-10-23 11:23:43 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service expired on 2021-10-23 11:23:43.
Certificate details:

fingerprint (SHA-1)	744EC6629479417277FAC6065186C28C136A921F
fingerprint (SHA-256)	0315B850391B42C84B8E8039DC1E944D262095C9567E84 ↪2B8F17205B69F4A33D
issued by	CN=localhost
public key algorithm	RSA
public key size (bits)	2048
serial	00A67EF443813499F3
signature algorithm	sha256WithRSAEncryption
subject	CN=localhost
subject alternative names (SAN)	None
valid from	2021-09-23 11:23:43 UTC
valid until	2021-10-23 11:23:43 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security

. . . continues on next page . . .

... continued from previous page ...

Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

[return to 20.44.214.63]

2.1.2 Medium 8444/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service expired on 2021-10-23 11:23:43.
Certificate details:

fingerprint (SHA-1)	744EC6629479417277FAC6065186C28C136A921F
fingerprint (SHA-256)	0315B850391B42C84B8E8039DC1E944D262095C9567E84 ↪2B8F17205B69F4A33D
issued by	CN=localhost
public key algorithm	RSA
public key size (bits)	2048
serial	00A67EF443813499F3
signature algorithm	sha256WithRSAEncryption
subject	CN=localhost
subject alternative names (SAN)	None
valid from	2021-09-23 11:23:43 UTC
valid until	2021-10-23 11:23:43 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)

NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost
Certificate details:

fingerprint (SHA-1)	744EC6629479417277FAC6065186C28C136A921F
fingerprint (SHA-256)	0315B850391B42C84B8E8039DC1E944D262095C9567E84 ↪2B8F17205B69F4A33D
issued by	CN=localhost
public key algorithm	RSA
public key size (bits)	2048
serial	00A67EF443813499F3
signature algorithm	sha256WithRSAEncryption
subject	CN=localhost
subject alternative names (SAN)	None
valid from	2021-09-23 11:23:43 UTC

... continues on next page ...

... continued from previous page ...

valid until	2021-10-23 11:23:43 UTC

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

[return to 20.44.214.63]

2.1.3 Medium 514/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service is signed by the following untrusted and/o

... continues on next page ...

... continued from previous page ...

```
↪r dangerous CA:
Issuer: CN=localhost
Certificate details:
fingerprint (SHA-1)              | 744EC6629479417277FAC6065186C28C136A921F
fingerprint (SHA-256)            | 0315B850391B42C84B8E8039DC1E944D262095C9567E84
↪2B8F17205B69F4A33D
issued by                        | CN=localhost
public key algorithm             | RSA
public key size (bits)           | 2048
serial                           | 00A67EF443813499F3
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=localhost
subject alternative names (SAN)  | None
valid from                       | 2021-09-23 11:23:43 UTC
valid until                      | 2021-10-23 11:23:43 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

... continues on next page ...

... continued from previous page ...

Summary
The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The certificate of the remote service expired on 2021-10-23 11:23:43.
Certificate details:
fingerprint (SHA-1)             | 744EC6629479417277FAC6065186C28C136A921F
fingerprint (SHA-256)           | 0315B850391B42C84B8E8039DC1E944D262095C9567E84
↪2B8F17205B69F4A33D
issued by                       | CN=localhost
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 00A67EF443813499F3
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost
subject alternative names (SAN) | None
valid from                      | 2021-09-23 11:23:43 UTC
valid until                     | 2021-10-23 11:23:43 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

[return to 20.44.214.63]

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: 2890363766
Packet 2: 2890364817
```

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
```

... continues on next page ...

... continued from previous page ...

```
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 20.44.214.63]
