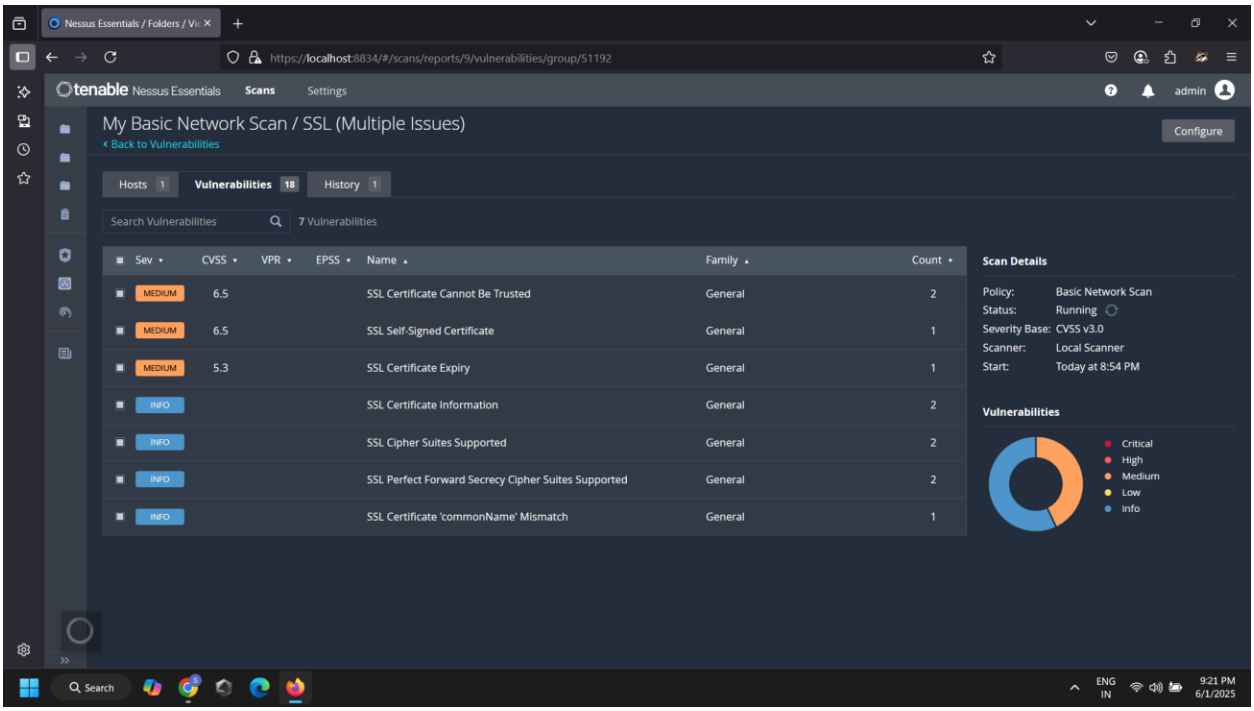
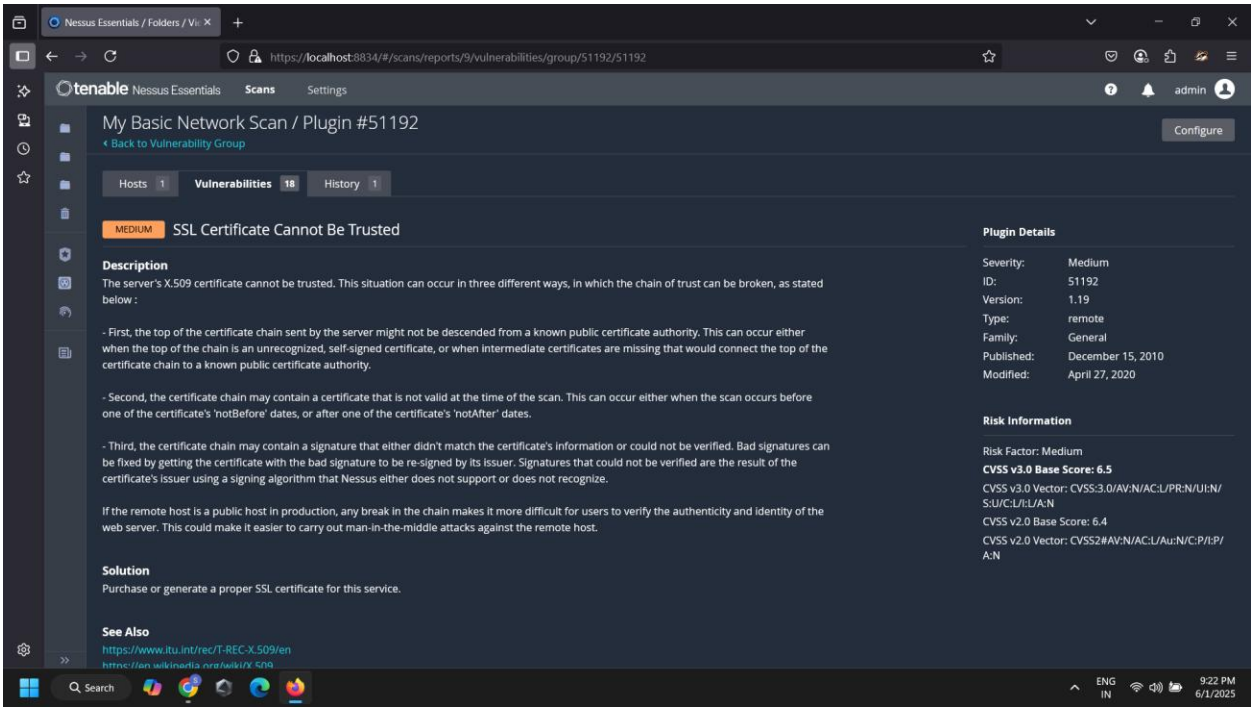
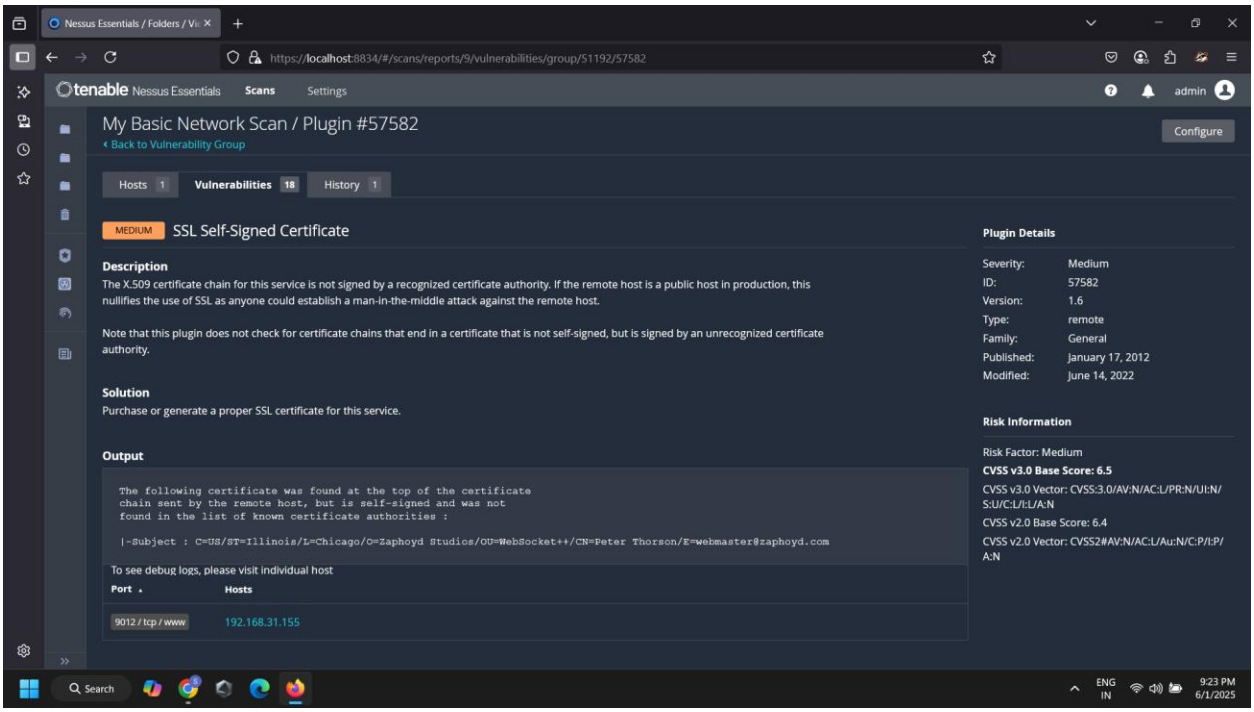
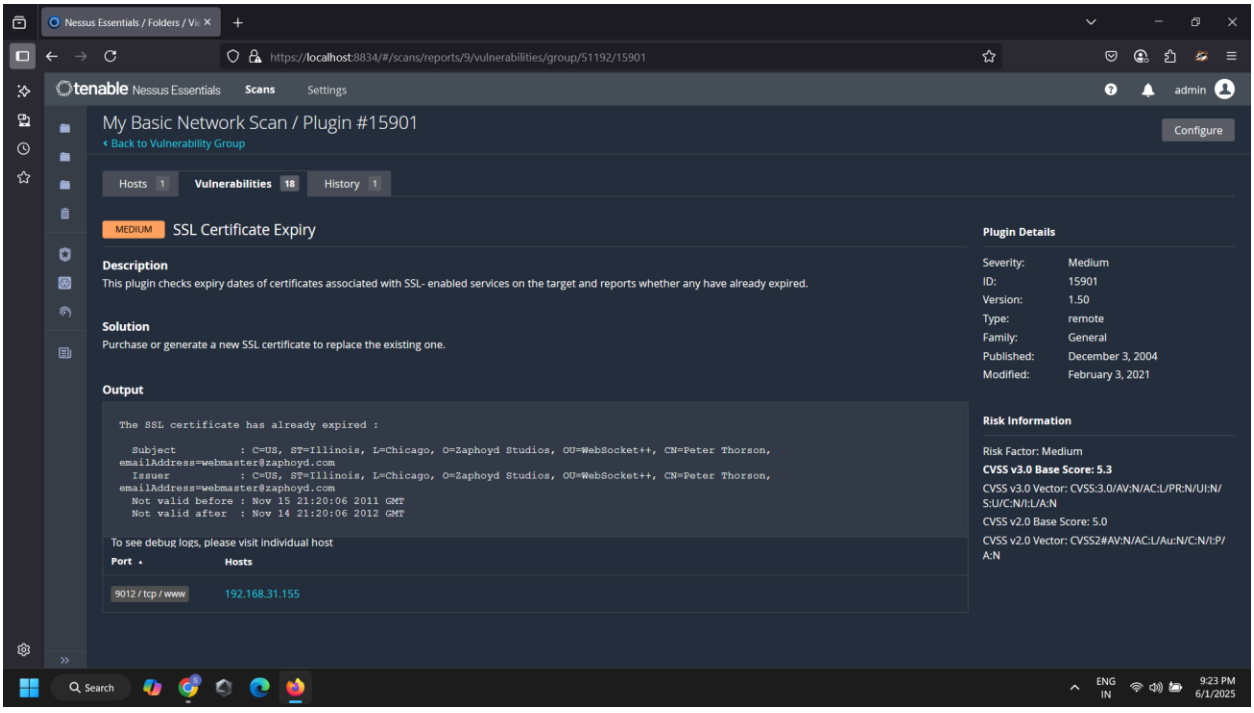
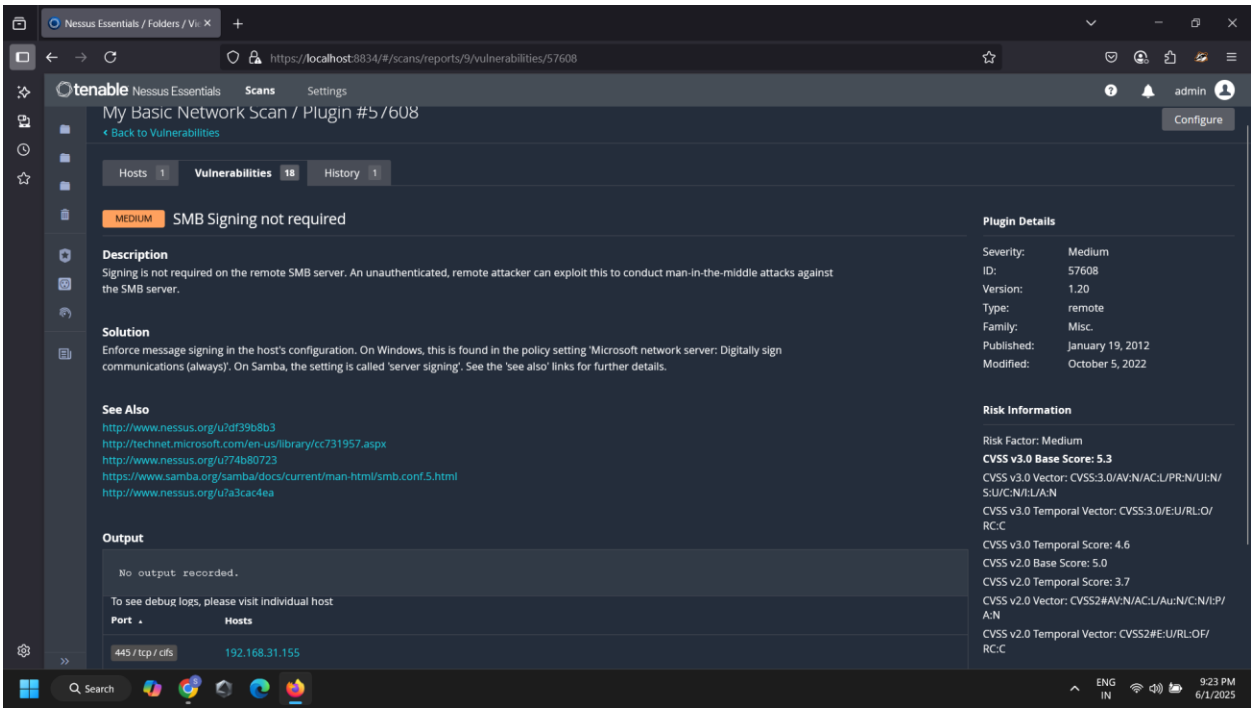

Nessus Essentials / Folders / Vi
https://localhost:8834/#/scans/reports/9/vulnerabilities/group/51192
tenable Nessus Essentials
Scans
Settings
admin
My Basic Network Scan / SSL (Multiple Issues)
Back to Vulnerabilities
Configure
Hosts 1
Vulnerabilities 18
History 1
Search Vulnerabilities
7 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MEDIUM 6.5 SSL Certificate Cannot Be Trusted General 2
MEDIUM 6.5 SSL Self-Signed Certificate General 1
MEDIUM 5.3 SSL Certificate Expiry General 1
INFO SSL Certificate Information General 2
INFO SSL Cipher Suites Supported General 2
INFO SSL Perfect Forward Secrecy Cipher Suites Supported General 2
INFO SSL Certificate 'commonName' Mismatch General 1
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:54 PM
Vulnerabilities
Critical
High
Medium
Low
Info
Search
ENG
IN
9:21 PM
6/1/2025


Nessus Essentials / Folders / Vi
https://localhost:8834/#/scans/reports/9/vulnerabilities/group/51192/51192
tenable Nessus Essentials
Scans
Settings
admin
My Basic Network Scan / Plugin #51192
Back to Vulnerability Group
Configure
Hosts 1
Vulnerabilities 18
History 1
MEDIUM SSL Certificate Cannot Be Trusted
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.
Solution
Purchase or generate a proper SSL certificate for this service.
See Also
https://www.itu.int/rec/T-REC-X.509/en
Plugin Details
Severity: Medium
ID: 51192
Version: 1.19
Type: remote
Family: General
Published: December 15, 2010
Modified: April 27, 2020
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score: 6.4
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N
Search
ENG
IN
9:22 PM
6/1/2025


Nessus Essentials / Folders / Vi
https://localhost:8834/#/scans/reports/9/vulnerabilities/group/51192/57582
tenable Nessus Essentials
Scans
Settings
admin
My Basic Network Scan / Plugin #57582
Back to Vulnerability Group
Configure
Hosts 1
Vulnerabilities 18
History 1
MEDIUM
SSL Self-Signed Certificate
Description
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.
Solution
Purchase or generate a proper SSL certificate for this service.
Output
The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :
|-Subject : C=US/ST=Illinois/L=Chicago/O=Zaphoyd Studios/OU=WebSocket++/CN=Peter Thorson/E=webmaster@zaphoyd.com
To see debug logs, please visit individual host
Port
Hosts
9012 / tcp / www
192.168.31.155
Plugin Details
Severity: Medium
ID: 57582
Version: 1.6
Type: remote
Family: General
Published: January 17, 2012
Modified: June 14, 2022
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score: 6.4
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N
Search
ENG IN
9:23 PM 6/1/2025


Nessus Essentials / Folders / Vi
https://localhost:8834/#/scans/reports/9/vulnerabilities/group/51192/15901
tenable Nessus Essentials
Scans
Settings
admin
My Basic Network Scan / Plugin #15901
Back to Vulnerability Group
Configure
Hosts 1
Vulnerabilities 18
History 1
MEDIUM
SSL Certificate Expiry
Description
This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.
Solution
Purchase or generate a new SSL certificate to replace the existing one.
Output
The SSL certificate has already expired :
Subject : C=US, ST=Illinois, L=Chicago, O=Zaphoyd Studios, OU=WebSocket++, CN=Peter Thorson, emailAddress=webmaster@zaphoyd.com
Issuer : C=US, ST=Illinois, L=Chicago, O=Zaphoyd Studios, OU=WebSocket++, CN=Peter Thorson, emailAddress=webmaster@zaphoyd.com
Not valid before : Nov 15 21:20:06 2011 GMT
Not valid after : Nov 14 21:20:06 2012 GMT
To see debug logs, please visit individual host
Port
Hosts
9012 / tcp / www
192.168.31.155
Plugin Details
Severity: Medium
ID: 15901
Version: 1.50
Type: remote
Family: General
Published: December 3, 2004
Modified: February 3, 2021
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
Search
ENG IN
9:23 PM 6/1/2025


Nessus Essentials / Folders / Vu
https://localhost:8834/#/scans/reports/9/vulnerabilities/57608
tenable Nessus Essentials
Scans
Settings
admin
My Basic Network Scan / Plugin #57608
Back to Vulnerabilities
Configure
Hosts 1
Vulnerabilities 18
History 1
MEDIUM
SMB Signing not required
Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
See Also
http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea
Output
No output recorded.
To see debug logs, please visit individual host
Port
Hosts
445 / tcp / cifs
192.168.31.155
Plugin Details
Severity: Medium
ID: 57608
Version: 1.20
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: October 5, 2022
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C
Search
ENG
IN
9:23 PM
6/1/2025