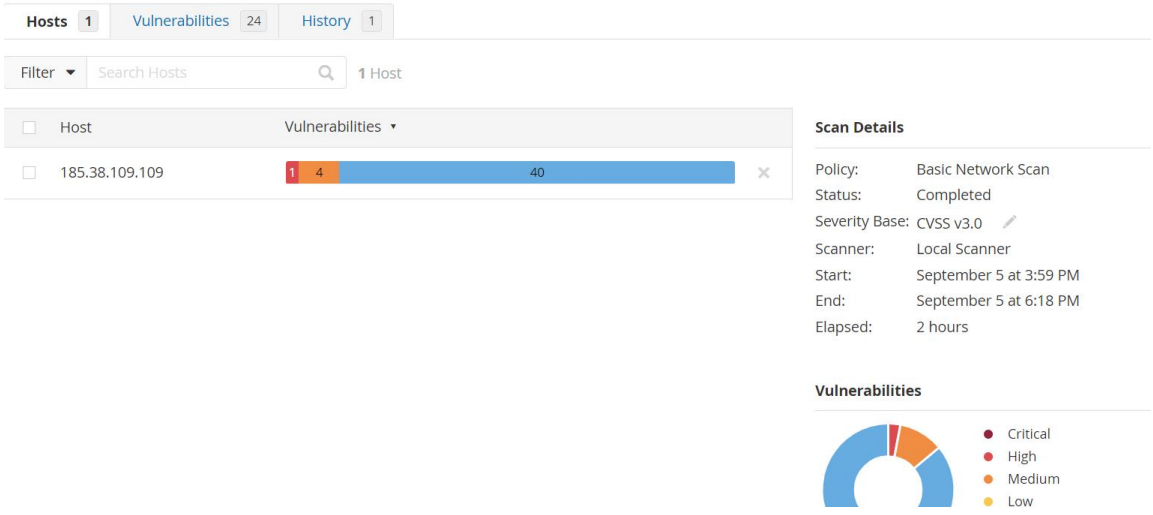
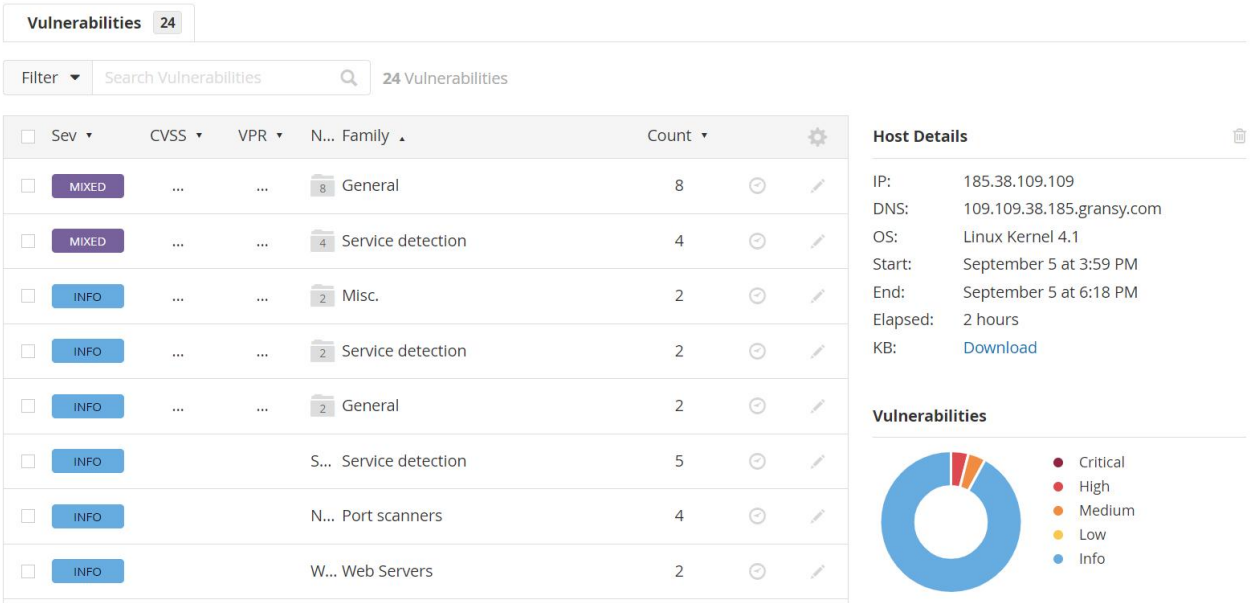
Name : Veekshitha
Reg no: 21BCE8943

TASK - 7 : NESSUS

Scan :



Vulnerabilities :



Vulnerabilities 24

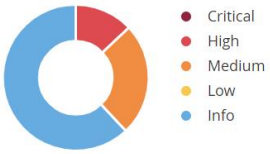
Search Vulnerabilities | 8 Vulnerabilities

Sev	CVSS	VPR	N...	Family	Count
HIGH	7.5	6.1	S...	General	1
MEDIUM	6.5		S...	General	1
MEDIUM	6.5		S...	General	1
INFO			S...	General	1
INFO			S...	General	1
INFO			S...	General	1
INFO			S...	General	1
INFO			S...	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	September 5 at 3:59 PM
End:	September 5 at 6:18 PM
Elapsed:	2 hours

Vulnerabilities



Vulnerabilities 24

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX          Auth     Encryption
MAC
    ----------------------        ----------        ---          ----     ----------
----------  ---
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH         RSA      3DES-
CBC(168)          SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA          RSA      3DES-
more...
```

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	185.38.109.109

Plugin Details

Severity:	High
ID:	42873
Version:	1.21
Type:	remote
Family:	General
Published:	November 23, 2009
Modified:	February 3, 2021

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events

CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.1
Risk Factor: Medium
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

Vulnerability Pub Date: August 24, 2016
In the news: true

Reference Information

CVE: CVE-2016-2183

Vulnerabilities 24

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.

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

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=*
|-Issuer  : CN=*
```

To see debug logs, please visit individual host

Port ▲	Hosts
443 / tcp / www	185.38.109.109

Vulnerabilities 24

MEDIUM TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Plugin Details

Severity:	Medium
ID:	104743
Version:	1.10
Type:	remote
Family:	Service detection
Published:	November 22, 2017
Modified:	April 19, 2023

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N

CVSS v2.0 Base Score: 6.1

CVSS v2.0 Vector:
CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N

Vulnerability Name : SSL Medium Strength Cipher Suites Supported (SWEET32)

Risk : High

CWE : (CWE-326)
This CWE ID is used to classify weaknesses related to the use of cryptographic algorithms and cipher suites that may be susceptible to attacks due to their insufficient strength or improper configuration.

Description :
SWEET32 refers specifically to the vulnerability where an attacker can exploit the use of 64-bit block ciphers in SSL/TLS cipher suites, leading to the possibility of collision attacks and information leakage.

OWASP :
SWEET32 is not explicitly listed in the OWASP Top Ten, it falls under the broader category of "Insecure Cryptographic Storage," which is a common concern addressed by OWASP.

Business Impact:
The business impact of the SWEET32 vulnerability can be significant. If exploited, it can lead to the compromise of sensitive data that is transmitted over SSL/TLS connections. This includes financial information, login credentials, personal data, or any other confidential information. Such a breach can result in reputational damage, legal consequences, and financial losses.

Remediation:

> Disable 64-bit Block Ciphers
> Update and Reconfigure
> Periodic Key Rotation

>Monitoring and Alerting
>Consider TLS 1.2 or Higher
>Use Security Best Practices

Vulnerability Name: SSL Certificate Cannot Be Trusted

Risk: Medium

CWE: (CWE-295)
This CWE ID is used to classify weaknesses related to SSL certificate issues, including expired certificates, self-signed certificates, or certificates signed by untrusted or unknown certificate authorities.

Description:
The SSL certificate cannot be trusted vulnerability occurs when a web server presents an SSL/TLS certificate that is either expired, self-signed, or signed by an untrusted or unknown certificate authority (CA). This means that the authenticity and security of the SSL/TLS connection cannot be verified, potentially exposing users to security risks.

OWASP: The issue of untrusted SSL certificates aligns with the broader category of "Broken Authentication" in the OWASP Top Ten. While OWASP does not specifically list SSL certificate trust issues, they emphasize the importance of secure authentication, which includes the use of valid and trusted SSL certificates to establish secure connections.

Business Impact: The business impact of the SSL certificate cannot be trusted vulnerability can be significant. It can erode user trust, lead to data breaches, and compromise sensitive information. Users may avoid using the affected website or application due to security concerns, resulting in a loss of reputation, potential legal consequences, and financial losses.

Remediation:

> Renew or Replace Certificates: Ensure that SSL/TLS certificates are valid and up to date. Renew or replace expired certificates promptly.

> Use Certificates from Trusted CAs.

Implement Certificate Monitoring: Set up a certificate monitoring system to proactively track certificate expiration dates and receive alerts for renewal.

Regularly Update CA Trust Stores: Keep the list of trusted certificate authorities up to date on the server to ensure trust in the certificates presented.

Implement HSTS (HTTP Strict Transport Security): Enable HSTS to ensure that browsers only connect to your site using HTTPS and avoid potential downgrade attacks.

Implement OCSP Stapling: Use OCSP stapling to improve the verification of certificate validity and reduce reliance on the CA's online status check.

Use Security Best Practices: Follow security best practices in configuring and managing SSL/TLS certificates and ensure their proper installation and configuration.