TEAM-7.5

NESSUS SCAN

Website: Spotify

TEAM MEMBERS :

HARSHIT RAJ

Pabbisetty Pranavi

Shivanshu Tiwari

LAKSHMI

1)Vulnerability name: TLS Version 1.0 Protocol Detection

CWE: 327

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.

Business Impact: TLS 1.0 is vulnerable to various attacks, including POODLE, BEAST, and CRIME, which can lead to data breaches and unauthorized access to sensitive information. Using this outdated protocol can put your business and your customers' data at risk.

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

Output

TLSv1 is enabled and the server supports at least one cipher.

2) Vulnerability name: SSL Certificate 'commonName' Mismatch

Description: The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Business Impact: One of the primary reasons for using SSL/TLS certificates is to ensure secure and encrypted communication between the user's browser and the website. When the CN does not match the domain, it can raise security concerns. Users may be hesitant to interact with a website they perceive as untrustworthy or potentially malicious.

Solution: If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Output:

The host name known by Nessus is :

25.224.186.35.bc.googleusercontent.com

The Common Name in the certificate is :

canary-certificate-for-noop.spotify.com

The Subject Alternate Name in the certificate is :

canary-certificate-for-noop.spotify.com

3) Vulnerability name: OS Identification

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Business Impact: While OS identification can be used for security benefits, it can also be exploited by malicious actors. If attackers can determine the OS of a target system, they may use this information to launch more targeted attacks or exploit known vulnerabilities for that OS.

Solution: Limit access to OS identification data to authorized personnel only. Implement access controls and authentication mechanisms to prevent unauthorized access.

Output:

Remote operating system : Microsoft Windows Server 2012 R2

Confidence level : 56

Method : MLSinFP

The remote host is running Microsoft Windows Server 2012 R2.

4) Vulnerability name: SSL Root Certification Authority Certificate Information

Description: The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

Business Impact: If a Root CA certificate is compromised or misused, it can lead to security breaches and loss of customer trust. This can have severe financial and reputational consequences for both the CA and the businesses relying on their certificates.

Solution: Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10

Output

The following root Certification Authority certificate was found :

|-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2

|-Issuer : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2

|-Valid From : Aug 01 12:00:00 2013 GMT

|-Valid To : Jan 15 12:00:00 2038 GMT

|-Signature Algorithm : SHA-256 With RSA Encryption

5) Vulnerability name: Web Server No 404 Error Code Check

Description: The remote web server is configured such that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate

Business impact: Hackers looking for web servers with poor handling of 404 errors may be attempting to identify vulnerabilities in the server or website. They could exploit these vulnerabilities to gain unauthorized access, steal data, or disrupt services.

Solution: Keep your web server software, content management system (CMS), and all related components up to date. Software updates often include security patches to address known vulnerabilities.

Output

CGI scanning will be disabled for this host because the host responds

to requests for non-existent URLs with HTTP code 301

rather than 404. The requested URL was :

http://25.224.186.35.bc.googleusercontent.com/ChnZsHC5gHJy.html