SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Web Security- IE2062

Insecure TLS Protocol Version Vulnerability

Danuka Nuwan

IT22349842

Title of Vulnerability: Insecure TLS Protocol Version Vulnerability

Description of Vulnerability:

The program sustains unconfident TLS technique variations such as SSLv2, SSLv3, or out-of-date variations of TLS (e.g., TLS 1.0 as well as TLS 1.1), which are susceptible to cryptographic strikes and also acknowledged susceptabilities.
Assaulters can make use of these weak points to block, decode, or damage secured interaction threatening the discretion plus stability of delicate information sent in between clients as well as web servers.

Website- temu.com

Components Affected:

SSL/TLS arranges Network interaction methods (e.g., HTTPS).

Assessment of Impact:

High: Insecure TLS process variations position a huge threat to the safety of the program, maybe bring about unapproved gain access to, information leakage, coupled with concession of vital info exchanged over the network.

Steps for Replicating:

Conduct a safety and security study of the application's SSL/TLS setups to discover sustained process modifications as well as cipher collections.

Take advantage of automated scanning devices or handson evaluation methods to discover unconfident TLS process variants, consisting of SSLv2, SSLv3, TLS 1.0 coupled with TLS 1.1.

Examine network website traffic making use of package smelling devices to obstruct secured contact also figure out the worked-out TLS method variation throughout the SSL/TLS handshake.

Examine the effect of outdated TLS method variations on the privacy as well as honesty of transferred information by trying cryptographic strikes such as downgrade strikes or method susceptabilities usage.

Verify the efficiency of TLS technique variation hardening actions by imposing the utilization of modern as well as safe and secure TLS variations throughout SSL/TLS setup.

Proof of Concept:

4. Insecure Transportation Security Protocol Supported (TLS 1.0)

LOW 1 CONFIRMED 1

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

4.1. https://temu.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```


- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf`file and remove `TLSv1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32`or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\T
LS 1.0\
```

    3. Locate a key named `Server`or create if it doesn't exist.
    4. Under the `Server`key, locate a DWORD value named `Enabled`or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

Suggested Solution:

Evaluation as well as update SSL/TLS configurations to avoid unconfident technique variations, con sisting of SSLv2, SSLv3, TLS 1.0, as well as TLS 1.1.

Set up internet servers, plenty balancers, as well as various other network gadgets to focus on maki ng use of modernday and also safe as well as secure TLS variations, such as TLS 1.2 as well as TLS 1.3.

Carry out secured cipher collection prioritizing to make sure that simply solid cryptographic formul ae as well as cipher collections are sustained throughout SSL/TLS settlement.

Allow Perfect Forward Secrecy (PFS) to ensure that session secrets are shortterm as well as not vul nerable to lucid security also if lasting personal tricks are jeopardized.

Consistently keep a watch on SSL/TLS arrangements as well as network web traffic for abnormal ha bits a symptom of prospective safety threats, including as downgrade attacks or process susceptab ilities exploitation.

Inform system managers including programmers on the significance of putting up safe SSL/TLS inte ractions moreover the hazards associated to unsafe approach variants.