SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Web Security- IE2062

Weak Ciphers

Danuka Nuwan

IT22349842

Title of Vulnerability: Weak Ciphers Enabled

Description of Vulnerability:

The application's interaction networks make use of poor cryptographic ciphers, subjecting delicate information to probable interception and also file encryption by assaulters.
Weak ciphers are prone to cryptographic strikes, such as strength recognized plaintext or man-in-the-middle attacks, endangering the privacy and also stability of delivered information.

Website- www.temu.com

Components Affected:

- SSL/TLS configurations
- Network communication protocols (e.g., HTTPS)

Assessment of Impact:

High: Weak ciphers making it possible for in the application's interaction networks position a big threat to information safety and security maybe leading in unapproved gain access to, information leakage as well as concession of delicate data.

Steps for Replicating:

Execute a protection examination of the application's SSL/TLS arrangements to determine the cipher collections and also security approaches being employed.

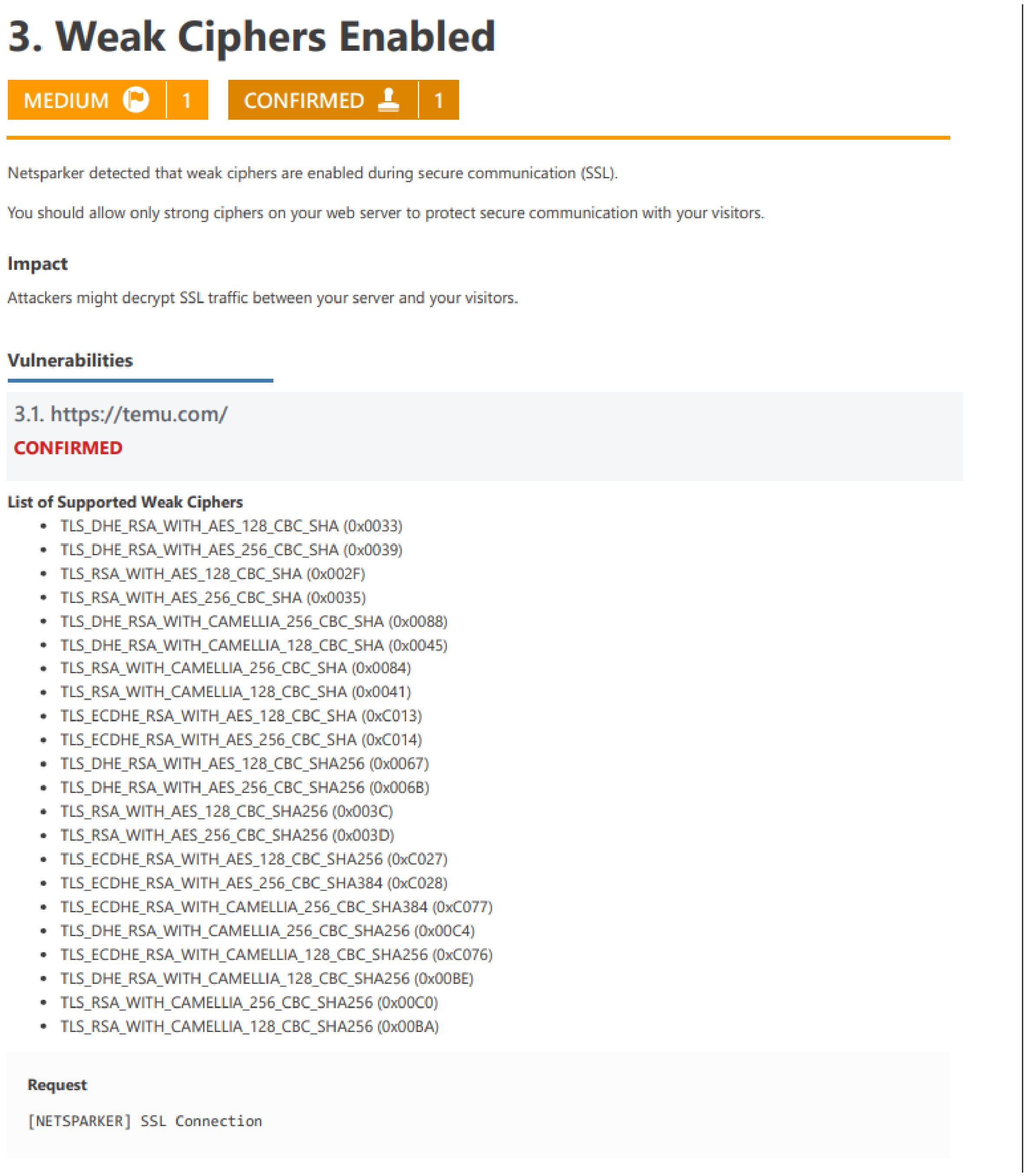
Make use of automated scanning devices or hand-operated evaluation tactics to detect weak cryptographic ciphers such as RC4, DES or older variations of SSL/TLS processes.

Examine network website traffic making use of package scenting devices to obstruct along with assess encrypted interaction determining employing poor ciphers.

Analyze the effect of weak ciphers on the privacy as well as stability of conveyed information by trying cryptographic strikes such as strength or recognized plaintext strikes.

Validate the efficiency of cipher configuration stages by trying to discuss increasingly powerful cipher collections throughout SSL/TLS handshake.

Proof of Concept:



3. Weak Ciphers Enabled

MEDIUM | 1 CONFIRMED | 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

3.1. https://temu.com/

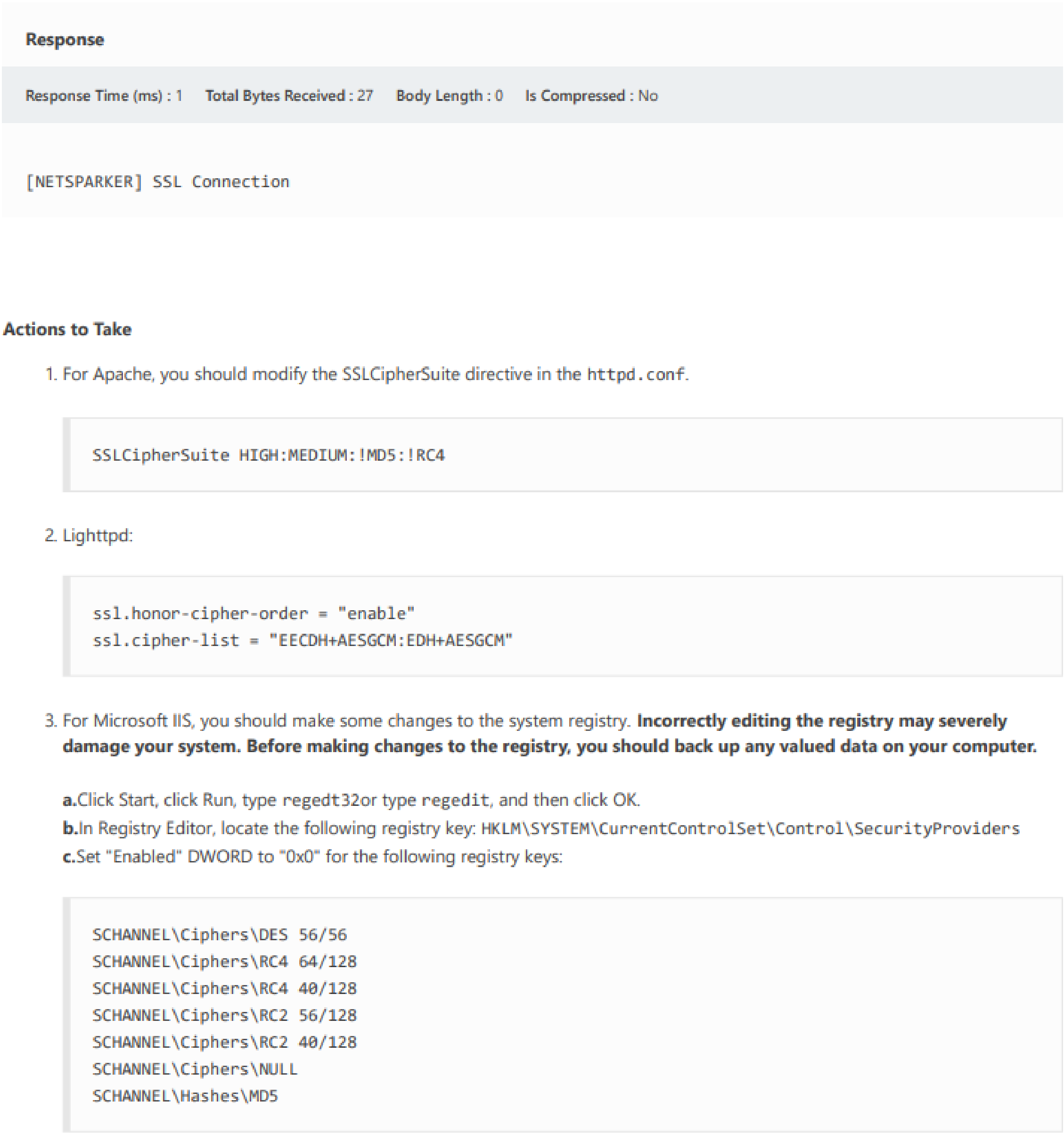
CONFIRMED

List of Supported Weak Ciphers

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xC077)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C4)
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xC076)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BE)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C0)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BA)

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

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to 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.**

a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

I found these weak ciphers on Temu.com web site.

Suggested Solution:

Evaluation and also upgrade SSL/TLS settings to disable weak cipher collections as well as deprecated security procedures consisting of SSLv2, SSLv3, and also TLS 1.0/ 1.1.

Allow Perfect Forward Secrecy (PFS) to make certain that session secrets are short-term and also not vulnerable to retroactive file encryption also if long-lasting exclusive secrets are jeopardized.

Use solid cryptographic formulas and also cipher collections suggested by safety and security ideal procedures such as AES-GCM, AES-CBC with HMAC and also Elliptic Curve Cryptography (ECC).

Carry out protected cipher collection prioritizing to make sure that one of the most safe and secure security techniques plus cipher collections are picked throughout SSL/TLS settlement.

Routinely book SSL/TLS setups along with cryptographic programs for conformance with sector standards and also finest techniques.

Display SSL/TLS handshake fails as well as cipher collection settlements for inexplicable habits a measure of prospective safety threats.

Inform system managers together with designers on the significance of putting up safeguarded SSL/TLS interactions as well as the hazards related with weak cryptographic ciphers.