Ubaid Jafri

DIGITAL CERTIFICATE ASSESSMENT

DISCLAIMER

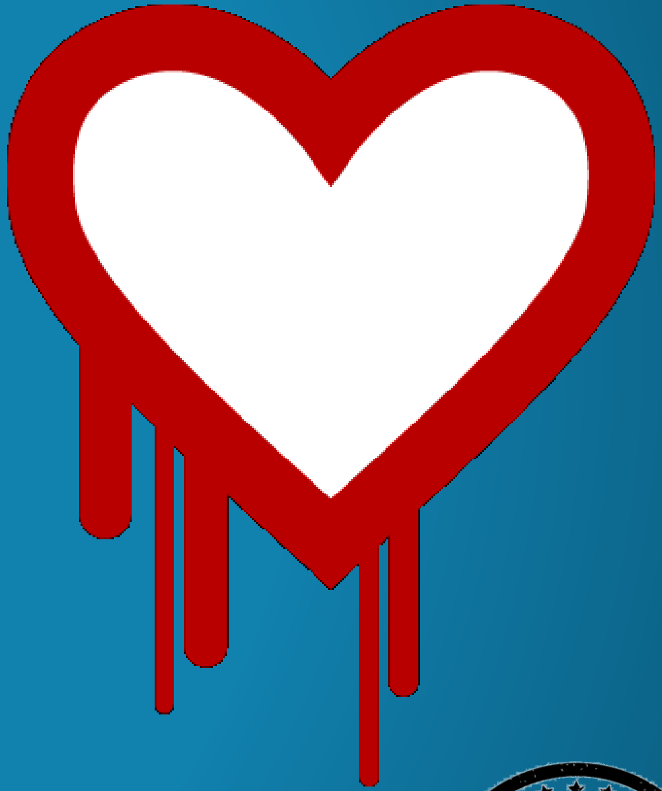
This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

Heart bleed vulnerability



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

HEARTBLEED VULNERABILITY

Description:

✓ The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

✓ The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

How to stop leakage?

✓ As long as the vulnerable version of OpenSSL is in use it can be abused. Fixed OpenSSL has been released and now it has to be deployed. Operating system vendors and distribution, appliance vendors, independent software vendors have to adopt the fix and notify their users. Service providers and users have to install the fix as it becomes available for the operating systems, networked appliances and software they use.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

BEAST VULNERABILITY

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

BEAST VULNERABILITY

Description:

- ✓ Short for Browser Exploit Against SSL/TLS, BEAST is a browser exploit against SSL/TLS that was revealed in late September 2011. This attack leverages weaknesses in cipher block chaining (CBC) to exploit the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol. The CBC vulnerability can enable man-in-the-middle (MITM) attacks against SSL in order to silently decrypt and obtain authentication tokens, thereby providing hackers access to data passed between a Web server and the Web browser accessing the server.

Mitigation:

- ✓ Disable TLS 1.0 and have users connect using TLS 1.1 or TLS 1.2 protocols which are immune to the BEAST attack. TLS 1.0 is now considered insecure and disabling the protocol improves the overall security of the SecureAuth IdP Appliance.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

POODLE VULNERABILITY

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

POODLE VULNERABILITY

Description:

- ✓ A POODLE attack is an exploit that takes advantage of the way some browsers deal with encryption. POODLE (Padding Oracle On Downgraded Legacy Encryption) is the name of the vulnerability that enables the exploit.

- ✓ POODLE can be used to target browser-based communication that relies on the Secure Sockets Layer (SSL) 3.0 protocol for encryption and authentication. The Transport Layer Security (TLS) protocol has largely replaced SSL for secure communication on the Internet, but many browsers will revert to SSL 3.0 when a TLS connection is unavailable. An attacker who wants to exploit POODLE takes advantage of this by inserting himself into the communication session and forcing the browser to use SSL 3.0.

Mitigation:

- ✓ It is recommended to upgrade certificates from SSLv2.0 to TLS encryption.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

CRIME VULNERABILITY

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

CRIME VULNERABILITY

Description:

- ✓ Compression Ratio Info-leak Made Easy (CRIME) is a security exploit against secret web cookies over connections using the HTTPS and SPDY protocols that also use data compression. When used to recover the content of secret authentication cookies, it allows an attacker to perform session hijacking on an authenticated web session, allowing the launching of further attacks.

- ✓ CRIME is a client-side attack, but the server can protect the client by refusing to use the feature combinations which can be attacked. For CRIME, the weakness is Deflate compression. This alert is issued if the server accepts Deflate compression

Mitigation:

- ✓ CRIME can be defeated by preventing the use of compression, either at the client end, by the browser disabling the compression of HTTPS requests, or by the website preventing the use of data compression on such transactions using the protocol negotiation features of the TLS protocol. As detailed in The Transport Layer Security (TLS) Protocol Version 1.2, the client sends a list of compression algorithms in its ClientHello message, and the server picks one of them and sends it back in its ServerHello message. The server can only choose a compression method the client has offered, so if the client only offers 'none' (no compression), the data will not be compressed. Similarly, since 'no compression' must be allowed by all TLS clients, a server can always refuse to use compression.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

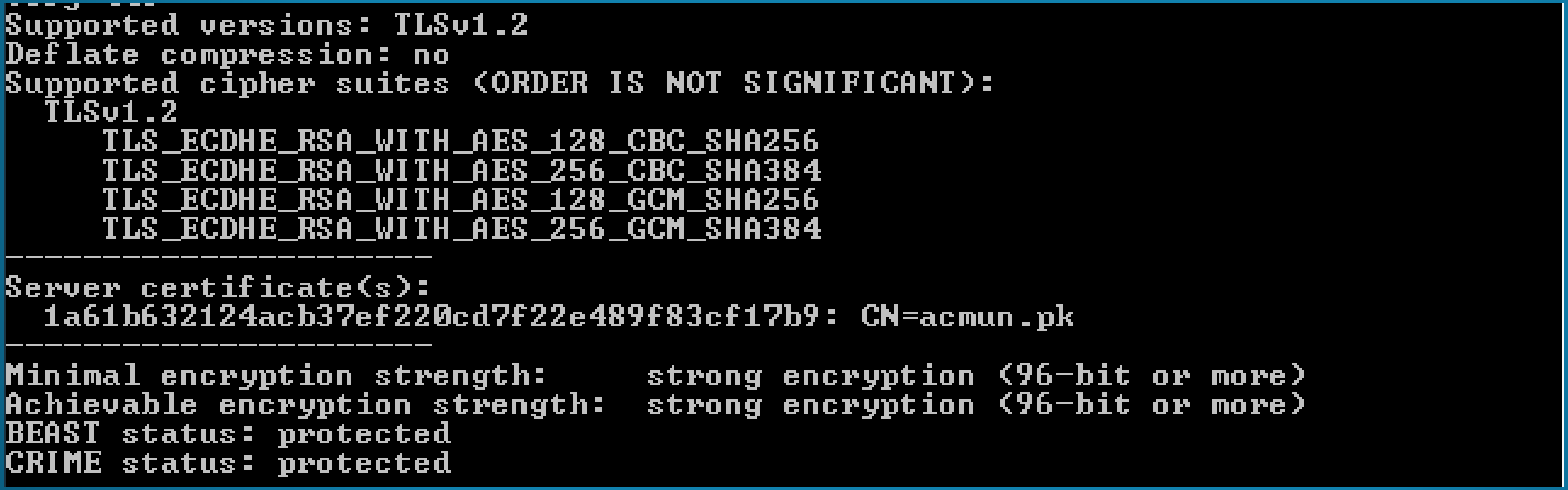
DEMONSTRATION

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

DEMONSTRATION

Run tool with

C:\ProgramFiles\java> java -jar TestSSLServer.jar <www.website.com> 443



```
Supported versions: TLSv1.2
Deflate compression: no
Supported cipher suites (ORDER IS NOT SIGNIFICANT):
  TLSv1.2
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
----------------------
Server certificate(s):
  1a61b632124acb37ef220cd7f22e489f83cf17b9: CN=acmun.pk
----------------------
Minimal encryption strength:     strong encryption (96-bit or more)
Achievable encryption strength:  strong encryption (96-bit or more)
BEAST status: protected
CRIME status: protected
```

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

THANK YOU

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.