crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

Soluzione

Disabilita SSLv2 e le suite di crittografia di livello di esportazione. Assicurati che le chiavi private non vengano utilizzate da nessuna parte con software server che supporti le connessioni SSLv2.

See Also

https://drownattack.com/
https://drownattack.com/drown-attack-paper.pdf

Output

- The remote host is affected by SSL DROWN and supports the following vulnerable cipher suites :

```
  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth
Encryption             MAC
    ----------------------        ----------       ---           ----
--------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA
RC2-CBC(40)            MD5       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA
RC4(40)                MD5       export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth
Encryption             MAC
    ----------------------        ----------       ---           ----
--------------------  ---
    RC4-MD5                       0x01, 0x00, 0x80 RSA           RSA
RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```