上一篇: Computer Science and Automation (INRIA)的安全研究人员在<u>TLS 1.2</u>协议的实现过程中发现一个新漏洞,并将该新型攻击命名为"<u>SLOTH</u>"。中间人攻击者可利用SLOTH以下列方法攻击加密流量:

- 1、解密加密的流量
- 2、冒充合法的客户端
- 3、冒充合法的服务器

之所以称之为SLOTH,是因为攻击者强迫目标使用弱的哈希算法,这是首例公开的针对TLS、IKE 共SSH协议的原像/碰撞攻击。本文主要介绍降级攻击的机制,以及应对措施。

TLS1.2签名哈希算法降级

过去,SSL/TLS协议中曾经出现漏洞,使攻击者强制客户端/服务器使用弱SSL/TLS协议版本和加密 套件。<u>POODLE</u>、<u>FREAK</u>和<u>Logjam</u>攻击均使用这种方法工作。但是SLOTH不同:它迫使客户端/ 服务器使用弱哈希算法,降低应对攻击的计算能力。主要有两种可能的降级攻击方式:

- 1、客户端:发生在客户端允许使用服务器端的弱哈希算法。在SLOTH攻击中, TLS 1.2协议的ServerKeyExchange报文的SignatureAndHashAlgorithm字段允许该降级攻击。
- 2、服务器端:发生在服务器端允许使用客户端的弱哈希算法。在SLOTH攻击中,TLS协议中的ClientCertificateVerify报文允许该降级攻击。

客户端TLS 1.2 MD5降级

在TLS 1.2之前版本协议中,没有客户端和服务器端协商签名和哈希算法的选项,通常使用MD5和 SHA1连接。TLS 1.2在ServerKeyExchange报文中引入了一个新的字段SignatureAndHashAlgor ithm,允许服务器指定客户端使用的签名和哈希算法,同样的,也允许攻击者强制客户端使用弱哈希算法。下面的过程展示了降级攻击的发生过程:

在握手的初期,客户端将Client Hello数据包发生给服务器;数据包中声明了服务器可以使用的签名和加密算法。然而,攻击者可以截获该数据包,并且向客户端发送一个要求更改算法的数据包,迫使客户端接受。至此,攻击者就开始了冒充目标服务器的攻击过程。图一所示为一个Client Hello数据包,其中没有可用的RSA-MD5算法。

```
    Random

  Session ID Length: 0
  Cipher Suites Length: 132

    ⊕ Cipher Suites (66 suites)

  Compression Methods Length: 1

⊕ Compression Methods (1 method)

  Extensions Length: 72
Extension: status_request

    ⊞ Extension: renegotiation_info

    ⊕ Extension: elliptic_curves

 Extension: ec_point_formats
    Type: signature_algorithms (0x000d)
    Length: 28
    Signature Hash Algorithms Length: 26

─ Signature Hash Algorithms (13 algorithms)

    □ Signature Hash Algorithm: 0x0401

        Signature Hash Algorithm Hash: SHA256 (4)
        Signature Hash Algorithm Signature: RSA (1)

    Signature Hash Algorithm: 0x0402

        Signature Hash Algorithm Hash: SHA256 (4)
        Signature Hash Algorithm Signature: DSA (2)

    □ Signature Hash Algorithm: 0x0403

        Signature Hash Algorithm Hash: SHA256 (4)
        Signature Hash Algorithm Signature: ECDSA (3)
    ☐ Signature Hash Algorithm: 0x0501
        Signature Hash Algorithm Hash: SHA384 (5)
```

回复 Client Hello数据库安全

位于客户端和服务器端之间的攻击者通过发送Server Hello、Certificate和Server Key Exchange数据包响应客户端请求。在Server Key Exchange中,攻击者使用RSA-MD5算法替换客户端实际指定的算法。

```
∃ Secure Sockets Laver

☐ TLSv1.2 Record Layer: Handshake Protocol: Server Hello

     Content Type: Handshake (22)
     version: TLS 1.2 (0x0303)
     Length: 61
   TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
     Content Type: Handshake (22)
     Version: TLS 1.2 (0x0303)
     Lenath: 205
   Handshake Protocol: Server Key Exchange
       Handshake Type: Server Key Exchange (12)
       Length: 201
     □ EC Diffie-Hellman Server Params
        Curve Type: named_curve (0x03)
        Named Curve: secp256r1 (0x0017)
        Pubkey Length: 65
        Pubkey: 0406ed3863c94c68bf67d89a7d9915ffbf7fbb9c2324ea8b...
          Signature Hash Algorithm Hash: MD5 (1)
          Signature Hash Algorithm Signature: RSA (1)
        Signature Length: 128
        Signature: 30f6ac57a48024dcd5207be49715ecacdc9124a6d585f914.
```

图二 Server Key Exchange中包含RSA-MD5算法的服务器响应

客户端接收到"服务器端"的响应,并最终使用弱哈希算法。随后,客户端再次发送Client Key Exchange响应,握手成功。

TCP	bb Yes	31391-443 [SYN] Seq=U Win=819Z Len=U MSS=140U WS=Z30 SACK_PERM=1
TCP	66 Yes	443+31591 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_
TCP	54 Yes	31591-443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
TLSv1	308 Yes	Client Hello
TCP	60 Yes	443→31591 [ACK] Seq=1 Ack=255 Win=65536 Len=0
TLSv1	871 Yes	Server Hello, Certificate, Server Key Exchange, Server Hello Done
TLSv1	129 Yes	Client Key Exchange
TCP	60 Yes	443+31591 [ACK] Seq=818 Ack=330 Win=65536 Len=0
W 0 3	JAF WAR	about although the control of the co

```
TLSV1 280 Yes Change Cipner Spec, Hello Kequest, Hello Kequest
TLSV1 280 Yes New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
TCP 54 Yes 31591-443 [ACK] Seq=381 Ack=1044 Win=64512 Len=0
```

图三 攻击者降级成功

TLS通道降级后,中间人攻击者就可以冒充服务器,解密所有加密的流量。

服务器端TLS 1.2 MD5降级

SLOTH攻击也可以反方向工作。攻击者可以冒充客户端并迫使服务器使用弱的签名和加密算法。

在握手开始时,客户端向服务器发送Client Hello数据包,位于服务器和客户端的攻击者可截获该数据包,并前向转发伪造的Client Hello数据包,且该数据包中只提供RSA-MD5算法。

```
∃ TLSv1 Record Layer: Handshake Protocol: Client Hello

    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
   Length: 107

⊟ Handshake Protocol: Client Hello

      Handshake Type: Client Hello (1)
      Length: 103
      Version: TLS 1.2 (0x0303)
   ⊞ Random
      Session ID Length: 0
      Cipher Suites Length: 14

    ⊕ Cipher Suites (7 suites)

      Compression Methods Length: 2

    Compression Methods (2 methods)

      Extensions Length: 47
    Extension: SessionTicket TLS
    ∃ Extension: signature_algorithms
        Type: signature_algorithms (0x000d)
        Length: 4
        Signature Hash Algorithms Length: 2

☐ Signature Hash Algorithms (1 algorithm)

        ☐ Signature Hash Algorithm: 0x0101
            Signature Hash Algorithm Hash: MD5 (1)
            Signature Hash Algorithm Signature: RSA (1)
```

图四 只提供RSA-MD5算法的Client Hello数据包

当然,中间人攻击者可以发送signature_algorithms字段中的附加数据,但是由于其中包含服务器不支持的值,服务器会忽略这些数据。在这种情况下,攻击者就可以冒充客户端,一旦TLS通道降级成功,就可以让TLS级别的客户端身份验证。

缓解措施

SLOTH攻击揭示了TLS协议的最新版本中的一些安全问题。即使在安全协议栈中禁用弱密码套件, 该攻击仍能发生。

在TLS 1.2以后的版本中, TLS协议实现中的许多响应都会删除MD5支持。因此, 在大多数情况下, 更新现有的TLS栈可以有效的解决此类问题。但是, 该更新操作不能仅限于TLS协议, 因为SS

H和VPN服务也会受到SLOTH攻击的影响。安全人员可以检查TLS、SSH和VPN相关的所有配置,并禁用MD5支持。同时,如果使用的是第三方通信设备,那么应该检查当前配置和供应商更新信息。

* 原文地址:<u>trendmicro</u>, vul_wish编译,转载请注明来自FreeBuf黑客与极客(FreeBuf.CO M)