

当您使用ASA和AnyConnect时，请避免长卷毛狗和长卷毛狗叮咬漏洞

TAC

文档ID118780

已更新：2015年5月06日

贡献用Atri巴苏，Cisco TAC工程师。



[下载 pdf文档](#)



[打印](#)

[反馈](#)

相关产品

- [Cisco AnyConnect VPN 客户端](#)
- [思科自适应安全设备 \(ASA\) 软件](#)
- [安全套接字层 \(SSL\)](#)
- [Cisco AnyConnect 安全移动客户端](#)
- [Cisco ASA 5500-X系列下一代防火墙](#)

目录

[简介](#)

[背景信息](#)

[问题](#)

[解决方案](#)

[TLSv1.2](#)

[相关信息](#)

[相关的思科支持社区讨论](#)

简介

本文描述什么您必须执行避免在Downgraded传统加密(长卷毛狗)漏洞的填充的Oracle，当您使用可适应安全工具(ASA)时和AnyConnect安全套接字协议层(SSL)连接。

背景信息

传输层安全版本1 (TLSv1)协议的长卷毛狗漏洞影响某些实施，并且可能允许未经鉴定，远端攻击者

访问敏感信息。

漏洞归结于在TLSv1实现的不正确的分组加密填充符，当您使用密码链块(CBC)时模式。攻击者能利用漏洞为了进行在密码消息的一“oracle填充符”旁拉信道攻击。成功的检测安全漏洞代码能允许攻击者访问敏感信息。

问题

ASA允许流入SSL连接以两种形式：

1. 无客户端WebVPN
2. AnyConnect Client

然而，在ASA的TLS实施或AnyConnect客户端都是没有受长卷毛狗的影响的。反而，SSLv3实施受影响，以便所有客户端(浏览器或AnyConnect)协商SSLv3是易受此漏洞。

警告：然而长卷毛狗叮咬影响在ASA的TLSv1。关于受影响的产品和修正的更多信息，参考[CVE-2014-8730](#)。

解决方案

思科实现这些解决方案对此问题：

1. 以前支持的所有版本AnyConnect (经过协商的) SSLv3贬抑，并且版本可以下载(v3.1x和v4.0)不会协商SSLv3，因此他们不是易受问题。
2. ASA的[默认协议设置](#)从SSLv3更改到TLSv1.0，以便，只要流入连接是从支持TLS的客户端，那是什么将协商。
3. ASA可以手工配置接受仅特定SSL协议用此命令：

[ssl server-version](#)

按照解决方案1所述，当前支持的AnyConnect客户端都不再协商SSLv3，因此客户端不能连接到任何ASA配置与这些命令之一：`ssl server-version sslv3`

`ssl server-version sslv3-only`

然而，使用v3.0.x和v3.1.x AnyConnect版本贬抑(是所有AnyConnect构建版本PRE

3.1.05182)的部署，并且在哪儿SSLv3协商特定使用，唯一的解决方案将排除使用SSLv3或考虑到客户端升级。

4. 长卷毛狗叮咬的(Cisco Bug ID [CSCus08101](#))实际修正将集成到仅最新的临时版本版本。您能升级到ASA有解决的修正问题的版本。在Cisco在线连接(CCO)的第一个可用的版本是版本9.3(2.2)。

此漏洞的第一个已修复ASA软件版本如下：

**8.2系列： 8.2.5.558.4系列： 8.4.7.269.0系列： 9.0.4.299.1系列： 9.1.69.2系列
： 9.2.3.39.3系列： 9.3.2.2**

TLSv1.2

- ASA支持TLSv1.2根据软件版本9.3(2)。
- AnyConnect版本4.x客户端全部支持TLSv1.2。

这意味着：

- 如果运行此软件版本或更加高的使用无客户端WebVPN，则所有ASA能协商TLSv1.2。
- 如果使用AnyConnect客户端，为了使用TLSv1.2，您将需要升级对版本4.x客户端。

相关信息

- [CVE-2014-8730](#)
- [Cisco Bug ID CSCug51375](#)
- [Cisco Bug ID CSCur42776](#)
- [技术支持和文档 - Cisco Systems](#)

本文档是否是有用？[有](#) [没有](#)

感谢您的反馈。

[打开支持案例](#)（需要[思科服务合同](#)。）

相关的思科支持社区讨论

[思科支持社区](#)是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 [Cisco Technical Tips Conventions](#)。

已更新：2015年5月06日

文档ID118780