目录

简介

本文描述在Downgraded传统加密(长卷毛狗)攻击的填充的Oracle在思科电子邮件安全工具(ESA)。

问题

安全套接字协议层(SSL)版本3.0 (RFC-6101)是过时和不安全协议。当对于多数实用的目的，它由其后继路由替换了-传输层安全(TLS)时版本1.0 (RFC-2246)， TLS版本1.1 (RFC-4346)和TLS版本1.2 (RFC-5246) -许多TLS实施向后保持？与SSL版本3.0兼容为了与老式系统兼容为了一平稳的用户体验。协议握手那么通常提供已验证版本协商，最新的协议版本普通对客户端，并且使用服务器。然而，即使客户端和服务器两个支持TLS版本， SSL版本3.0提供的安全等级是否是相关的，因为许多客户端实现协议降级舞蹈为了在服务器附近工作？旁边互通性Bug。

攻击者能利用降级舞蹈和中断SSL版本3.0口令安全。长卷毛狗攻击给他们，例如，窃取？安全？HTTP Cookie (或其他持票人令牌例如HTTP授权报头内容)。

此漏洞分配普通的漏洞和风险(CVE) ID CVE-2014-3566。

解决方案

这是相关Bug列表：

- Cisco Bug ID CSCur27131 - SSL版本3.0在ESA (CVE-2014-3566)的长卷毛狗攻击
- Cisco Bug ID CSCur27153 - SSL
- Cisco Bug ID CSCur27189 - SSL
- Cisco Bug ID CSCur27340 - SSL

在非联邦信息处理的标准(FIP)模式， SSL版本3.0在默认设置启用。默认情况下在FIPS模式，SSL版本3.0禁用。为了检查FIP模式是否启用，请输入：

```
CLI> fipsconfig

FIPS mode is currently disabled.
```

当FIP模式禁用时，请检查SSL版本3.0是否在sslconfig设置启用。当sslv3列出作为方法时， SSL版

本3.0启用。更改此对TLS版本1为了禁用SSL版本3.0。

```
CLI> sslconfig
sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: <cipher list>
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: <cipher list>
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: <cipher list>
example.com> sslconfig

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> GUI

Enter the GUI HTTPS ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the GUI HTTPS ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
 GUI HTTPS method:  tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> INBOUND

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3
```

```
Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
 GUI HTTPS method:  tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> OUTBOUND

Enter the outbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the outbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
 GUI HTTPS method:  tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>

example.com> commit

Please enter some comments describing your changes:
[]> remove SSLv3 from the GUI HTTPS method/Inbound SMTP method/Outbound SMTP method

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Thu Oct 16 07:41:10 2014 GMT
```

相关信息

- CVE-2014-3566
- 谷歌announcment
- Openssl announcment
- 技术支持和文档 - Cisco Systems