目录

简介

某非 Cisco 来源发布了对 Cisco 配置文件中的用户口令（及其他口令）进行解密的程序。对于用 **enable secret** 命令设置的口令，该程序无法解密。此程序在 Cisco 用户中导致了意外的恐慌。这使我们意识到，许多依赖于 Cisco 口令加密的用户想要获得更高的安全性，但其最初设计所能提供的安全性有所不足。本文解释在Cisco密码加密后的安全模式和该加密安全限制。

注意： 思科建议所有Cisco IOS设备实现验证、授权和统计(AAA)安全模式。AAA 可以使用本地、RADIUS 和 TACACS+ 数据库。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

用户密码

用户密码和多数其他密码(*不是***enable secret**)在Cisco IOS配置文件加密使用由现代密码标准是非常弱的方案。

虽然思科不分配解密程序， Cisco IOS密码的至少两个不同的解密程序供给在互联网的公共;思科知道这样程序的第一个公共版本是在1995年初。我们会盼望所有业余译解密码者能创建与一点努力的一个新的程序。

Cisco IOS的方案用于用户密码未曾打算抵抗一确定的，智能攻击。加密机制设计通过简单监听或探测避免密码盗窃。未曾打算防止受到执行在配置文件的某人一密码破解努力。

由于弱加密算法，总是思科的位置客户应该对待包含密码的所有配置文件作为敏感信息，以与他们会对待密码相似的方式明文列表。

enable secret和特权密码

应该不再使用**enable password命令**。请使用 **enable secret** 命令以获得更高的安全性。**enable password命令**也许测试的唯一的实例是，当设备在不支持**enable secret命令的**boot模式时运行。

使用MD5算法， Enable secret被切细。只要任何人在思科知道，是不可能的恢复根据配置文件的内容的enable secret (除由明显的词典攻击之外)。

注意： 这仅适用对密码设置**enable secret**和*不于*密码设置**特权密码**。的确，使用的加密的优点是两命令之间的唯一的重大的差异。

哪Cisco IOS镜像支持enable secret ？

查看您的启动镜像使用**show version命令**从您的正常操作模式(全双工Cisco IOS镜像)发现启动镜像是否支持**enable secret命令**。如果它，删除**特权密码**。如果启动镜像不支持**enable secret**，请注释以下警告：

- 设置特权密码也许是多余的，如果有物理安全，以便没人能重新加载设备到启动镜像。
- 如果某人访问物理访问设备，他能容易地推翻设备安全性，无需需要访问启动镜像。
- 如果设置**特权密码**对同**enable secret一样**，您使**enable secret**一样倾向攻击作为**特权密码**。
- 如果对在ROM偶尔地使用不支持**enable secret命令的**一个不同的值的集**特权密码，**因为启动镜像不支持**enable secret**，您的路由器管理员必须记住新密码。由有一分开的特权密码，管理员可能不记住密码，当他们强制软件升级的时停机时间，是唯一的原因登陆到boot模式。

其他密码

几乎所有密码和其他认证字符串在Cisco IOS配置文件加密使用用于用户密码的弱，可逆方案。

要确定哪方案用于加密一个特定密码，请检查先于在配置文件的位加密的字符串。如果该位是7，使用弱算法，密码加密。如果位是5，使用更加强的MD5算法，密码被切细了。

例如，在配置命令：

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

enable secret切细了与MD5，而在命令：

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

使用弱可逆算法，密码加密。

配置文件

当您发送在电子邮件时的配置信息，您应该清洁从类型7密码的配置。您能使用**show tech-support命令**，默认情况下清洁信息。示例**show tech-support命令output**如下所示。

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

当保存您的在简单文件传输协议(TFTP)服务器时的配置文件，请更改在该文件的权限，当不是在使用中或放置它在防火墙后时。

算法能更改？

思科没有立即规划支持Cisco IOS用户密码的一种更加强的加密算法。如果思科应该决定在将来介绍这样功能，该功能明确地将强加另外的管理负担给选择利用它的用户。

换成用户密码马里兰-是，一般情况，不可能的用于enable secret，因为MD5是单向散列函数和密码的基于算法不可能从已加密数据恢复。为了支持某一身份验证协议(值得注意地CHAP)使用可逆算法，对用户密码明文的系统需要访问，并且必须存储他们。

密钥管理问题将做它一重要任务转换到一种更加强的可逆算法，例如DES。虽然修改Cisco IOS使用DES加密密码是容易的，这样做没有安全好处，如果所有Cisco IOS系统使用了同一DES密钥。若不同不同的系统使用密钥，管理负担为所有Cisco IOS网络管理员将介绍，并且将损坏配置文件的轻便在系统之间的。更加强的可逆密码加密的客户需求小。

相关信息

- 密码恢复规程
- 硬化Cisco IOS设备的Cisco指南
- 技术支持 - Cisco Systems