在SX350X或SX550X交换机的安全引导程序

目标

此条款目的将解释Secure引导程序进程，方法启动与只委托软件。此功能是启用的开始与固件版本2.4.0.91。

可适用的设备

SX350X

SX550X

软件版本

2.4.0.91

简介

安全引导程序是加载和运行方式一安全镜像使用一系列信任避免装载不信任软件。一系列信任的A通过分配与专用密钥的镜像和使用硬件与软件机制验证加载的镜像设立。当他们负荷设备固件，没有添加了一安全违犯代码时的其他人这允许用户是肯定的。

当用户设法装载一新的镜像时，新的镜像下载到临时文件，验证。在错误的情况下，临时文件删除。这样，如果新的镜像无效，安装过程将发生故障并且表示警告消息。

如果您的交换机在堆叠拓扑里

当您装载2.4.0.91，或者新版本联机，在主控交换机上，将装载在堆叠的所有成员的固件。不管在家族内的型号这是，因为它是要求所有设备运行同样固件。堆叠通常将作用。

安全启动程序

在启动期间，系统将打印在终端的安全启动信息。这是设备通过检查得，在安全引导程序前的步骤。

*引导程序只读存储器(BootROM)*验证*booton*

*Booton*验证通用引导程序(*Uboot)*

*Uboot*验证*ROS镜像*

如果安全引导程序检测失败，将防止设备启动。如果这发生，在这种情况下请与您的Cisco合作伙伴或技术支持中心(TAC)联系确定以下步骤跟随。如果需要找到Cisco合作伙伴，请点击此处。

获取引导程序Syslog

在启动期间，系统将打印安全启动信息：

安全引导程序启用/禁用–在没有系统在芯片(SoC)电子可编程的保险丝(eFuse)的设备，例如最小系统(MSYS)中央处理器(CPU)，或者，当eFuse巩固时位没有设置，打印输出将是“获取禁用的引导程序”。如果安全引导程序启用，打印输出将是“获取启用的引导程序”。

在*BootROM*验证*booton后*，打印验证状态(*通过/失败*)。

在*booton*验证*Uboot后*，打印验证状态(*通过/失败*)。

在*Uboot*验证*ros镜像后*，打印验证状态(*通过/失败*)。

注意：在失败的情况下，启动程序将终止。

巩固引导程序输出示例固件版本2.4.0.91 ：

```
                                BootROM - 1.73
Booting from NAND flash, Secure modeBootROM: RSA Public key verification PASSED
                    BootROM: CSK block signature verification PASSED
                  BootROM: Boot header signature verification PASSED
                        BootROM: Flash ID verification PASSED
                        BootROM: Box ID verification PASSED
                              BootROM: JTAG is enabled
                      General initialization - Version: 1.0.0
          AVS selection from EFUSE disabled (Skip reading EFUSE values)
                      Overriding default AVS value to: 0x23
                              Detected Device ID 6811
                          High speed PHY - Version: 2.0
                    :** Link is Gen1, check the EP capability
          PCIe, Idx 0: Link upgraded to Gen2 based on client capabilities
                        High speed PHY - Ended Successfully
                      DDR3 Training Sequence - Ver TIP-1.55.0
        DDR3 Training Sequence - Switching XBAR Window to FastPath Window
                  DDR3 Training Sequence - Ended Successfully
                  BootROM: Image checksum verification PASSED
               BootROM: Boot image signature verification PASSED
                           efuse secure mode: ON

               Aldrin ROS Booton: Oct 29 2017 13:42:52 ver. 2.0

                        Press x to choose XMODEM...
                          Booting from NAND flash
                         verify secure U-Boot pass
                             Running UBOOT...

U-Boot 2013.01 (Oct 29 2017 - 13:42:35) Marvell version: 2016_T1.0.eng_drop_v10 2.4.24
```

巩固引导程序输出示例固件版本2.5.0.83 ：

```
BootROM - 1.73
Booting from NAND flash, Secure modeBootROM: RSA Public key verification PASSED
BootROM: CSK block signature verification PASSED
BootROM: Boot header signature verification PASSED
BootROM: Flash ID verification PASSED


General initialization - Version: 1.0.0
AVS selection from EFUSE disabled (Skip reading EFUSE values)
Overriding default AVS value to: 0x23
Detected Device ID 6811
High speed PHY - Version: 2.0

Init Customer board mvHwsPexConfig: Link is Gen1, check the EP capability
PCIe, Idx 0: Link upgraded to Gen2 based on client capabilities
High speed PHY - Ended Successfully
DDR3 Training Sequence - Ver TIP-1.55.0
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED
BootROM: Boot image signature verification PASSED


Armada38x Booton: Apr 17 2018 21:23:48 ver. 2.1.3
efuse secure mode: ON

Press x to choose XMODEM...
Booting from NAND flash
Verify secure U-Boot pass
Running UBOOT...


U-Boot 2013.01 (Jun 18 2019 - 16:47:25) Marvell version: 2016_T1.0.eng_drop_v10 2.5.18

Loading system/images/active-image ...
Verify ROS secure Image pass, efuse is programmed
Uncompressing Linux... done, booting the kernel.
I2C frequency 100 kHz (Tclk 200 MHz, freq_m 12, freq_n 3)
```

结论

您当前熟悉安全引导程序，并且如何可帮助保护您的网络。