网真SUDI证书链安全扫描结果故障排除

目录

问题

安全漏洞扫描正在标记思科网真视频编解码器终端上与SSL/TLS证书相关的发现，特别是报告TCP端口4053、4060和4062上不受信任的证书链。漏洞扫描程序识别编解码器提供由ACT2 SUDI CA(组织：Cisco)，证书链终止于思科根CA 2048。安全扫描系统将此报告为不满足组织安全要求的不可信证书链。

安全扫描报告的具体结果包括：

- 自签名证书检测
- 不受信任的证书链
- 弱散列算法问题
- 证书到期警告

环境

- 思科网真视频编解码器终端
- 具有本地注册的Webex Desk系列设备
- 带有ACT2 SUDI（安全唯一设备标识符）芯片的终端
- 标记证书链问题的安全漏洞扫描基础设施
- TCP端口4053、4060和4062提供SUDI证书

分辨率

思科网真终端上的SUDI证书是嵌入的、不可变的证书，不能以受支持的方式修改、重新生成或删除。这些证书是Cisco Trustworthy Technologies实施的一部分，用于特定安全功能。

了解SUDI证书行为

证书行为因端口和系统配置而异：

- 端口4053（配对服务）：当系统具有ACT2芯片时，使用SUDI证书。自定义证书仅用于没有ACT2芯片（旧端点）的系统。
- 端口 4047：使用客户选择的证书在触摸面板和编解码器之间进行通信。

证书位置和详细信息

SUDI证书位于设备的证书存储区中：

```
device:~] $ cd /etc/cacerts_sudi
device:/etc/cacerts_sudi] $ ls
0763c37d.0                9426d327.0                mic-cbasrcarsa4k2099.pem
29cf4e89.0                a094437b.0                mic-cmca.pem
36087b08.0                b35c8d6c.0                mic-cmca2.pem
417aa245.0                cmca2.pem                 mic-cmca3.pem
771a09b9.0                crca2048.pem              mic-cmca4.pem
89087fe6.0                crca2099.pem              mic-crcam2.pem
90359431.0                mic-cbarc2099.pem         mic-harsa-ca.pem
```

ACT2 SUDI CA证书详细信息：

```
CN = ACT2 SUDI CA
O = Cisco
Valid From: Thursday, June 30, 2011 11:26:57 PM
Valid To: Tuesday, May 15, 2029 1:55:42 AM
```

推荐的操作

步骤 1：检查SUDI证书用途和安全实施

SUDI证书不是自签名证书，而是由思科制造CA签署。它充当不变的身份凭证，具有以下功能：

- 维护产品标识符和序列号
- 为配置、安全、审计和管理提供不可更改的身份
- 以加密方式绑定到信任锚模块芯片
- 使克隆或欺骗几乎不可能

步骤 2：与安全团队合作排除SUDI证书结果

由于无法修改SUDI证书并提供合法的安全功能，因此推荐的方法是：

- 配置安全扫描工具以排除受影响服务的SUDI证书链查找结果
- 根据思科的Trustworthy Technologies实施记录例外项的业务合理性
- 如果需要，将安全扫描重点放在其他端口上的客户可配置证书上

步骤 3：通过软件升级进行证书更新

当系统升级到更新的软件版本时，信任存储中的证书更新会自动发生。这可确保证书的有效性会随着时间推移而得到保持。

重要限制

以下限制适用于SUDI证书：

- 无法修改、重新生成或删除
- 如果删除证书并重新启动设备，则会自动重新生成
- 不存在将可配置证书分配给这些后端服务的受支持方法
- 由于信任锚点实施的不可变性质，无法替换证书

原因

安全扫描结果由思科的SUDI（安全唯一设备标识符）证书触发，这些证书是链接到思科根CA 2048的嵌入式制造证书。这些证书是Cisco Trustworthy Technologies实施的一部分，出于安全目的设计为不可变。组织安全扫描工具不会将证书识别为受信任，因为它们终止于思科的根证书颁发机构，而不是组织特定的CA。这是启用SUDI的设备的预期行为，代表设计功能而非安全漏洞。

相关内容

- Cisco Trustworthy Technologies数据表
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。