Ca-certificates删除不安全根证书

Base-service sig

问题背景

ca-certificates组件中被质疑包含不被信任的TrustCor Systems证书签发机构签发的根证书，包括TrustCor RootCert CA-1、TrustCor RootCert CA-2、TrustCor ECA-1，oE社区同样受影响。

问题详情：

TrustCor Systems机构在2022年，被媒体报出该公司和间谍软件供应商、A国情报界的公司有明显的联系，且该公司未给出有力的证据澄清这一事情，因此该CA机构的信任问题遭到业界质疑；

其它社区如Mozilla、Microsoft、Android、Ubuntu、Apple、openSUSE、Redhat等涉及到该CA机构证书的社区，已经将TrustCor Systems机构列为不被信任的根证书签发机构，并将该CA机构所签发的相关证书从系统中删除。

参考链接：

[1] https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/oxX69KFvsm4

[2] https://learn.microsoft.com/zh-cn/security/trusted-root/2023/feb2023

[3] https://android.googlesource.com/platform/system/ca-certificates

[4] https://ubuntu.com/security/notices/USN-5761-1

[5] https://support.apple.com/zh-cn/HT213645

[6] https://www.suse.com/support/update/announcement/2023/suse-su-20230037-1/

[7] https://access.redhat.com/security/cve/CVE-2022-23491

[8] https://trustcor.com/resources/trustcor-root-certificates.php

安全委员会11.1评审结论：

参照业界通用做法，删除所有版本中存在的不安全根证书

4、议题四：Ca-certificates删除不安全根证书 --王江、张晨峰

结论：参照业界通用做法，删除所有版本中存在的不安全根证书

https://gitee.com/src-openeuler/ca-certificates/issues/I87XH0

------调研证书使用的客户群

------2203-SP3/2003-SP4以及LTS都需要删除

------TC的议题增加改进策略

事件回放：

新闻及NVD

2022.09~2022.10

TrustCor Systems证书签发机构被媒体报出该公司和间谍软件供应商、美国情报界的公司有明显的联系，疑似是美国国防部的马甲

2022.11

涉及隐私研究的教授发表问题在google讨论区，社区开发者及部分用户逐渐关注此方面证书失信问题

2022.12

NVD发布了CVE-2022-23491（归属python-certifi包），该CVE描述中明确标明删除TrustCor公司的根证书。

2023.8

NVD发布了CVE-2023-21265（归属Android），该CVE描述了需要禁用根证书。修复方案与ca-certificates有关，删除对应证书

主流社区/厂商

2023.02

Apple发布安全公告，告知用户三个证书不安全，计划在2024年删除

2023.05

Ubuntu发布新版本软件包，新版中不安全证书已被删除

2023.08

openSUSE发布新版本软件包，已删除不安全证书

2023.10

Mozilla更新列表，在未来版本计划删除不安全证书

2024.x

Apple删除不安全证书
Mozilla删除不安全证书

OE

python-certifi包中包含三个不安全证书与ca软件包中不安全证书一致

2022.12

该CVE归属python-certifi包，并在gitee社区上创建了issue（https://gitee.com/src-openeuler/python-certifi/issues/I65DF7）
因软件包上游社区尚未有对应措施，同时申请挂起

CVE-manage针对推送过来漏洞信息刷新未提交新的issue关联组件

2023.08

python-certifi包升级到2023.07.22版本修复CVE，删除对应不安全证书，并关闭对应issue

2023.10

10.13 ca软件包完成issue创建
10.20 OE版本CCB会议评审
10.25 TC例会评审
11.1 上OE安全委员会例会评审
11月初 发布公告，更新CA证书包

删除后的影响分析

应用场景：

ca-certificates软件包作为所有受信任根证书集，主要用于系统在和其它服务器进行SSL/TLS连接时，验证服务器身份和安全性。该过程会使用服务器证书，通过证书链逐级验证到根证书（顶级证书），若系统内存在该根证书，则整条证书信任链完整，该服务器证书验证通过。

场景举例：当在Linux系统中，通过wget命令访问某https网站时，则会在建立连接期间，通过本地系统内的根证书去验证该网站证书。

影响分析：

删除相关不安全根证书，并不会对所有业务访问造成影响。只有当其它服务器部署了涉及该机构的证书，则证书校验时会验证到该机构的根证书。但因系统内该机构根证书已删除，则会导致验证失败而无法访问服务。

若用户涉及 TrustCor 机构根证书校验的情况，证书删除后可通过以下方法弥补：

1. 管理员可更换其它受信任CA机构签发的证书部署。
2. 若用户坚持访问，支持自行导入该CA机构的根证书。将下载好的根证书放在/etc/pki/ca-trust/source/anchors目录下，然后执行 /usr/bin/update-ca-trust 命令更新系统证书信任策略。

根证书官网下载地址：https://trustcor.com/resources/trustcor-root-certificates.php。

后续改进措施

分类	描述	责任团队	计划时间
漏洞感知	**Vtopia漏洞感知系统增加映射关系：**对python-ca软件包与ca证书包关联性进行分析后，发现软件包证书部分存在重复证书代码，后续将将两个软件包的CVE推送增加映射关系，对涉及的CVE进行同步分析。	安全委员会	已闭环
	SBOM成分分析增加证书内容：对内部软件包Sbom进行适配调整，将类似python-ca软件包与ca证书软件包问题进行关联分析，在其中一个软件包出现安全问题后，进行一系列涉及关联的软件包进行进一步排查。	社区基础设施-刘政均	11.30
	Cve-manage支持刷新机制：对vtopia刷新推送过来的CVE，如果影响范围扩大，支持在新的受影响仓库创建issue	社区基础设施-杨伟	11.30
漏洞修复	社区无补丁挂起漏洞跟踪：制定策略月度针对挂起漏洞进行跟踪，提醒漏洞owner关注是否有新的修复方案	安全委员会	11.30

THANKS