VSRC 安全周报（2021-07-27）

0x00 本周漏洞综述

本周需要关注漏洞共 7 个：Juniper Networks SBR 远程代码执行漏洞（CVE-2021-0276）；飞塔 FortiManager & FortiAnalyzer 远程代码执行漏洞（CVE-2021-32589）；惠普 & 施乐 & 三星打印机本地权限提升漏洞（CVE-2021-3438）；Linux Kernel 本地权限提升漏洞（CVE-2021-33909）；Redis 远程代码执行漏洞（CVE-2021-32761）;D-Link DIR-3040 路由器多个安全漏洞；Oracle 7 月多个安全漏洞。

本周安全态势共 1 个：绕过 macOS 的 TCC 用户隐私保护。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Juniper Networks SBR 远程代码执行漏洞（CVE-2021-0276）

漏洞概况

CVE ID	CVE-2021-0276	时 间	2021-07-19
类 型	RCE	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	无
PoC/EXP		在野利用	否

漏洞详情

2021 年 7 月 14 日，Juniper Networks 发布安全公告，其 Steel-Belted Radius Carrier Edition（SBR 运营商版）中存在一个远程代码执行漏洞（CVE-2021-0276），其 CVSS 评分为 9.8。

电信运营商通过 SBR 管理用户访问其网络的策略，通过集中用户认证、提供适当的访问级别并确保遵守安全策略。它使运营商能够提供差异化的服务水平，并管理网络资源。

由于配置了 EAP（可扩展认证协议）身份认证的 Juniper Networks SBR 中存在一个基于堆栈的缓冲区溢出漏洞，攻击者可以利用此漏洞发送特定的数据包，导致 radius 守护进程崩溃，从而造成拒绝服务（DoS）或远程代码执行（RCE）。

成功利用此漏洞将导致电信提供商（包括无线运营商）面临网络服务中断或其它风险。但该漏洞仅在使用增强型 EAP 日志和 TraceLevel 设置为 2 时影响配置了 EAP 身份验证的 SBR。

```
<SBR_Installed_Directory>/JNPRsbr/radius/radius.ini
[Logging]
LogLevel=2
TraceLevel=2
EnhancedEAPLogging = yes
```

影响范围

8.4.1 版本：< 8.4.1R19

8.5.0 版本：< 8.5.0R10

8.6.0 版本：< 8.6.0R4

安全建议

目前此漏洞已经修复，建议及时更新至 SBR Carrier 8.4.1R19、8.5.0R10、8.6.0R4 或更高版本。

下载链接：

https://support.juniper.net/support/downloads/

参考链接：

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11180&cat=SIRT_1&actp=LIST

https://threatpost.com/critical-juniper-bug-dos-rce-carrier/167869/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0276

2.飞塔 FortiManager & FortiAnalyzer 远程代码执行漏洞（CVE-2021-32589）

漏洞概况

CVE ID	CVE-2021-32589	时 间	2021-07-20
类 型	RCE	等 级	高危
远程利用	是	影响范围	
攻击复杂度	高	可用性	高

用户交互	无	所需权限	无
PoC/EXP	未公开	在野利用	否

漏洞详情

2021 年 7 月 19 日，Fortinet（飞塔）发布安全公告，修复了其 FortiManager 和 FortiAnalyzer 中的一个远程代码执行漏洞（CVE-2021-32589），该漏洞的 CVSS 评分为 7.5。

FortiManager 是 Fortinet 公司的一个集中管控设备，可以通过它集中管理任意数量的 Fortinet Network Security 设备。FortiAnalyzer 是 Fortinet 公司的集中日志分析解决方案，它可以汇聚 Fortinet 设备和第三方设备的日志或告警信息，为客户提供一个简化的、统一的安全管理分析平台。

由于 FortiManager 和 FortiAnalyzer 的 fgfmsd 守护进程中存在 Use–After- Free 漏洞（当程序将一段内存标记为空闲，但随后试图使用该内存时，会出现 UAF，这可能导致程序崩溃），未经身份验证的远程攻击者可以通过向目标设备的 fgfm 端口发送恶意请求来触发此漏洞，最终能够以 root 身份执行任意代码。

但需要注意的是，FortiAnalyzer 上的 FGFM 默认是禁用的，只能在特定硬件型号上启用：1000d、 1000e、2000e、3000d、3000e、 3000f、3500e、3500f、3700f、3900e。

安全建议

目前此漏洞已经修复，建议参考下表及时升级更新：

产品	受影响版本	修复版本

FortiManage	FortiManager 5.6.10 及以下版本。	升级到 FortiManager 5.6.11 或更高版本。
	FortiManager 6.0.10 及以下版本。	升级到 FortiManager 6.0.11 或更高版本。
	FortiManager 6.2.7 及以下版本。	升级到 FortiManager 6.2.8 或更高版本。
	FortiManager 6.4.5 及以下版本。	升级到 FortiManager 6.4.6 或更高版本。
	FortiManager 7.0.0 版本。	升级到 FortiManager 7.0.1 或更高版本。
	FortiManager 5.4.x 版本。	/
产品	受影响版本	修复版本
FortiAnalyzer	FortiAnalyzer 5.6.10 及以下版本。	升级到 FortiAnalyzer 5.6.11 或更高版本。
	FortiAnalyzer 6.0.10 及以下版本。	升级到 FortiAnalyzer 6.0.11 或更高版本。
	FortiAnalyzer 6.2.7 及以下版本。	升级到 FortiAnalyzer 6.2.8 或更高版本。
	FortiAnalyzer 6.4.5 及以下版本。	升级到 FortiAnalyzer 6.4.6 或更高版本。

	FortiAnalyzer 7.0.0 版。	升级到 FortiAnalyzer 7.0.1 或更高版本。

修复方法

使用以下命令在 FortiAnalyzer 设备上禁用 FortiManager 功能：

```
config system global
set fmg-status disable <--- 默认禁用
end
```

下载链接：

https://www.fortinet.com/cn

参考链接：

https://www.fortiguard.com/psirt/FG-IR-21-067

https://us-cert.cisa.gov/ncas/current-activity/2021/07/19/fortinet-releases-security-updates-fortimanager-and-fortianalyzer

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32589

3. 惠普 & 施乐 & 三星打印机本地权限提升漏洞（CVE-2021-3438）

漏洞概况

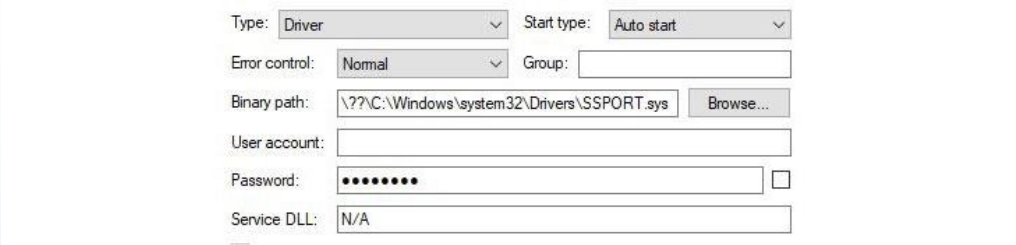
CVE ID	CVE-2021-3438	时 间	2021-07-21
类 型	LPE	等 级	高危
远程利用	否	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	低
PoC/EXP		在野利用	否

漏洞详情

2021 年 7 月 20 日，SentinelOne 公开披露了在 HP、Xerox 和 Samsung 打印机驱动程序中发现的一个存在了 16 年的本地权限提升漏洞（CVE-2021-3438），该漏洞影响了全球数亿台设备和数百万用户，其 CVSS 评分为 8.8。

由于 SSPORT.SYS 驱动程序中存在缓冲区溢出漏洞，攻击者可以利用此漏洞实现本地权限提升。据表示，存在漏洞的驱动程序会自动与打印机软件一起安装，并在系统每次重启后被 Windows 加载。即使在打印机未连接到目标设备的情况下，该漏洞也可能被滥用，且无需用户交互。

成功利用此漏洞的攻击者能够将权限提升到 SYSTEM 并在内核模式下运行代码，并可以安装程序、查看、更改、加密或删除数据，或者创建具有完全用户权限的新帐户。



影响范围

380 种型号的惠普和三星打印机

Xerox® B205/B210/B215

Xerox® Phaser® 3020/3052/3260/3320

Xerox® WorkCentre® 3025/3215/3225/3315/3325

注：受影响的打印机型号列表请参考惠普和施乐的安全公告。

安全建议

目前此漏洞已经修复。

鉴于漏洞的影响范围为较广，且利用复杂度低，建议相关用户参考官方公告及时升级更新，以避免被恶意利用或攻击。

下载链接：

惠普、三星：

https://support.hp.com/us-en/document/ish_3900395-3833905-16/hpsbpi03724

施乐：

https://securitydocs.business.xerox.com/wp-content/uploads/2021/05/cert_Security_Mini_Bulletin_XRX21K_for_B2XX_PH30xx_3260_3320_WC3025_32xx_33xx.pdf

参考链接：

https://labs.sentinelone.com/cve-2021-3438-16-years-in-hiding-millions-of-

printers-worldwide-vulnerable/

https://www.bleepingcomputer.com/news/security/16-year-old-bug-in-printer-software-gives-hackers-admin-rights/

https://thehackernews.com/2021/07/16-year-old-security-bug-affects.html

4. Linux Kernel 本地权限提升漏洞（CVE-2021-33909）

漏洞概况

CVE ID	CVE-2021-33909	时 间	2021-07-21
类 型	LPE	等 级	高危
远程利用		影响范围	
攻击复杂度		可用性	
用户交互		所需权限	
PoC/EXP	已公开	在野利用	

漏洞详情

2021 年 7 月 20 日，Qualys 研究团队公开披露了在 Linux 内核文件系统层中发现的一个本地提权漏洞（CVE-2021-33909，也称为 Sequoia）和 systemd（PID 1）中的一个拒绝服务漏洞（CVE-2021-33910）。

Linux Kernel 本地提权漏洞（CVE-2021-33909）

Linux 内核文件系统层中存在 size_t-to-int 类型转换漏洞。由于 fs/seq_file.c 没有正确限制 seq 缓冲区分配，从而导致整数溢出、越界写入以及权限提升。攻击者可以在默认配置中利用此漏洞，最终可以在受影响主机上获得 root 权限。该漏洞影响了自 2014 年以来发布的所有 Linux 内核版本。

影响范围

Linux kernel 3.16 - 5.13.x（5.13.4 之前）

Systemd(PID 1)拒绝服务漏洞（CVE-2021-33910）

systemd 是包含在大多数基于 Linux 系统中的软件套件，它提供了一个系统和服务管理器，作为 PID 1 运行并启动系统的其余部分。

该漏洞由 systemd v220（2015 年 4 月）提交的 7410616c（“核心：返工单元名称验证和操作逻辑”）引入，该漏洞将堆中的 strdup()替换为堆中的 strdupa()。何非特权用户都可以利用此漏洞使 systemd 崩溃，从而使整个系统崩溃（内核崩溃），导致拒绝服务。该漏洞影响了 2015 年 4 月之后发布的所有 systemd 版本。

影响范围

systemd 220 – 248

安全建议

目前这些漏洞已经修复。鉴于漏洞的影响范围较广，且 PoC 已经公开，建议受影响的用户尽快升级至 Linux Kernel 5.13.4（于 2021 年 7 月 20 日发布）或更高版本。

下载链接：

https://www.kernel.org/

参考链接：

https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/sequoia-a-local-privilege-escalation-vulnerability-in-linuxs-filesystem-layer-cve-2021-33909

https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/cve-2021-33910-denial-of-service-stack-exhaustion-in-systemd-pid-1

https://www.bleepingcomputer.com/news/security/new-linux-kernel-bug-lets-you-get-root-on-most-modern-distros/

5. Redis 远程代码执行漏洞（CVE-2021-32761）

漏洞概况

CVE ID	CVE-2021-32761	时 间	2021-07-22
类 型	RCE	等 级	高危
远程利用	是	影响范围	
攻击复杂度	高	可用性	高
用户交互	无	所需权限	低
PoC/EXP	未公开	在野利用	

漏洞详情

Redis 是一个开源的高性能 key-value 数据库，它在世界范围内被广泛应用。

2021 年 7 月 22 日， Redis 发布安全公告，公开了 Redis 32 位版本中的一个远程代码执行漏洞（CVE-2021-32761），该漏洞的 CVSSv3 评分为 7.5。

在 32 位系统上，Redis BITFIELD 命令存在整数溢出漏洞，通过修改默认的 proto-max-bulk-len 配置参数并构建特制的 bit 命令，攻击者可以破坏堆、泄漏任意堆内容或远程执行代码。该漏洞仅影响 32 位版本的 Redis。

影响范围

Redis >=2.2 and < 5.0.13

Redis >=2.2 and < 6.0.15

Redis >=2.2 and < 6.2.5

安全建议

目前此漏洞已经修复。建议及时更新至 Redis 6.2.5、6.0.15、5.0.13 或更高版本。

下载链接：

https://github.com/redis/redis

参考链接：

https://github.com/redis/redis/security/advisories/GHSA-8wxq-j7rp-g8wj

https://github.com/redis/redis

https://nvd.nist.gov/vuln/detail/CVE-2021-32761

6. D-Link DIR-3040 路由器多个安全漏洞

漏洞概述

2021 年 7 月 15 日，Cisco Talos 的研究人员公开披露了 D-Link DIR-3040 路由器中的多个安全漏洞，攻击者可以利用这些漏洞在受影响的路由器上执行任意代码、访问敏感信息或导致设备崩溃。目前这些漏洞的 PoC 已经公开。

漏洞详情

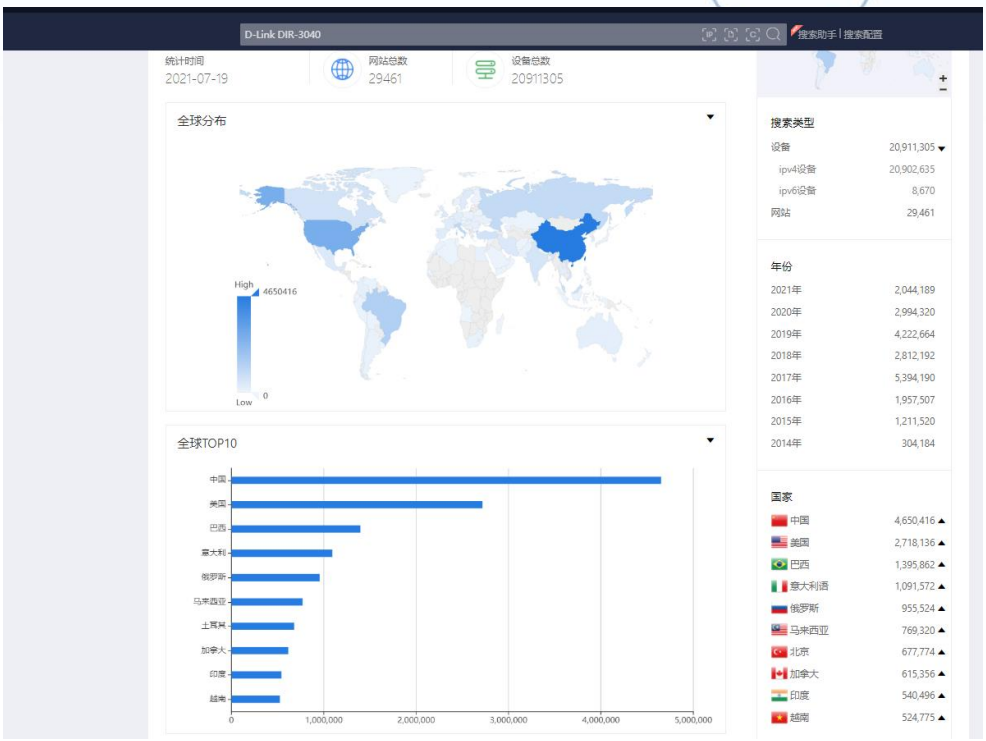
DIR-3040 是基于 AC3000 的无线互联网路由器。Cisco Talos 本次披露的漏洞包括：

- CVE-2021-21816 ： Syslog 信息泄露漏洞，CVSS 评分为 6.5。
- CVE-2021-21817 ： Zebra IP 路由管理器信息泄露漏洞，CVSS 评分为 7.5。
- CVE-2021-21818 ： Zebra IP 路由管理器硬编码密码漏洞，CVSS 评分为 7.5。
- CVE-2021-21819 ： Libcli 命令注入漏洞，CVSS 评分为 9.1。
- CVE-2021-21820 ： Libcli 测试环境硬编码密码漏洞，CVSS 评分为 10.0。

其中，CVE-2021-21816 和 CVE-2021-21817 为信息泄露漏洞，可通过恶意网络请求触发，成功利用可以查看设备的系统日志；CVE-2021-21819 漏洞可能导致任意命令执行，攻击者可以通过发送一系列请求来触发此漏洞。

CVE-2021-21818 和 CVE-2021-21820 都为硬编码密码漏洞，但影响不同，前者可能导致拒绝服务，后者可能导致攻击者在路由器上执行代码。

截止目前，通过 ZoomEey 搜索，全球范围内共搜索到 20911305 个 D-Link DIR-3040 相关的设备，其中中国位列第一，国内分布最多的为福建省。



影响范围

D-Link DIR-3040 固件 <= v1.13B03

安全建议

目前这些漏洞已经修复，建议及时应用 D-Link DIR-3040 v1.13B03 补丁。

下载链接：

https://support.dlink.com/resource/SECURITY_ADVISEMENTS/DIR-3040/REVA/DIR-3040_REVA_FIRMWARE_v1.13B03_HOTFIX.zip

参考链接：

https://blog.talosintelligence.com/2021/07/vuln-spotlight-d-link.html

https://supportannouncement.us.dlink.com/announcement/publication.aspx?

name=SAP10228

https://www.bleepingcomputer.com/news/security/d-link-issues-hotfix-for-hard-coded-password-router-vulnerabilities/

7. Oracle 7 月多个安全漏洞

漏洞概述

2021 年 7 月 20 日，Oracle 发布了 7 月份的安全更新，本次发布的安全更新共计 342 个，涉及 Oracle Communications Applications 、Oracle E-Business Suite、Oracle Enterprise Manager 和 Oracle Fusion Middleware 等多个产品和组件。

漏洞详情

Oracle Fusion Middleware 多个安全漏洞

Oracle 此次共发布了 48 个适用于 Oracle Fusion Middleware 的安全更新，其中有 35 个漏洞无需经过身份验证即可远程利用。其中包括多个 WebLogic Server 安全漏洞，未经身份验证的攻击者可以通过 IIOP 或 T3 协议发送恶意请求来利用这些漏洞，从而在 Oracle WebLogic Server 执行代码或控制服务器。严重漏洞包括 CVE-2021-2394、CVE-2021-2397 和 CVE-2021-2382，它们的 CVSS 评分均为 9.8。

Oracle Communications Applications 多个安全漏洞

Oracle 此次共发布了 33 个适用于 Oracle Communications Applications 的安全更新，其中有 22 个漏洞无需经过身份验证即可远程利用。其中严重漏洞包括 CVE-2021-21345、CVE-2020-11612、CVE-2021-3177、CVE-2020-17530 和 CVE-2019-17195，攻击者可以通过 HTTP 协议发送恶意请求来利用这些漏洞。

Oracle E-Business Suite 多个安全漏洞

Oracle 此次共发布了 17 个适用于 Oracle E-Business Suite 的安全更新，其中有 3 个漏洞无需经过身份验证即可远程利用。其中一个评级为严重的漏洞为 CVE-2021-2355（CVSS 评分为 9.1），该漏洞的利用复杂度低，且无需用户交互。此外，Oracle 还修复了包括 CVE-2021-2436、CVE-2021-2359 和 CVE-2021-2361 在内的 15 个高危漏洞。

Oracle Enterprise Manager 多个安全漏洞

Oracle 此次共发布了 8 个适用于 Oracle Enterprise Manager 的安全更新，这些漏洞都可以在未经过身份验证的情况下远程利用。其中一个评级为严重的漏洞为 CVE-2020-10683（CVSS 评分为 9.8），该漏洞的利用复杂度低，且无需用户交互。此外，Oracle 还修复了包括 CVE-2019-5064 在内的其它 7 个安全漏洞。

Oracle Financial Services Applications 多个安全漏洞

Oracle 此次共发布了 22 个适用于 Oracle Financial Services Applications 的安全更新，其中有 17 个漏洞无需经过身份验证即可远程利用。其中严重漏洞包括 CVE-2021-21345、CVE-2019-0228、CVE-2021-26117、CVE-2020-5413、CVE-2020-11998 和 CVE-2020-27218，攻击者可以通过 HTTP 协议发送恶意请求来利用这些漏洞。

安全建议

目前 Oracle 已发布相关安全更新，建议用户尽快修复。

下载链接：

https://www.oracle.com/security-alerts/cpujul2021.html

缓解措施

禁用 T3 协议：

1) 进入 WebLogic 控制台，在 base_domain 的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

2)在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：127.0.0.1 * * allow t3t3s，0.0.0.0/0 * *deny t3 t3s(t3 和 t3s 协议的所有端口只允许本地访问)。

3）保存后需重新启动，规则方可生效。

禁用 IIOP 协议:

登陆 WebLogic 控制台，base_domain >服务器概要 >AdminServer

参考链接:

https://www.oracle.com/security-alerts/cpujul2021.html

https://us-cert.cisa.gov/ncas/current-activity/2021/07/20/oracle-releases-july-2021-critical-patch-update

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2394

0x02 本周安全态势

1. 绕过 macOS 的 TCC 用户隐私保护

执行摘要

TCC 旨在保护用户数据免遭未经授权的访问，但其在设计上的弱点导致保护措施很容

易在无意中被绕过。TCC 不会阻止进程读取和写入“受保护”的位置，这是一个可用于隐藏恶意软件的漏洞。目前已知多个部分或完整的 TCC 绕过，至少有一个在野外被积极利用。此外，Automation 从设计上来说，存在全盘访问“后门”，同时也降低了授权障碍。

介绍

近年来，保护设备上的敏感数据变得越来越重要，特别是现在我们的手机、平板电脑和计算机被用来创建、存储和传输关于我们最敏感的数据：从照片和视频到密码、银行卡信息、健康和医疗数据以及社交出行等各种内容。

借助 macOS，Apple 早期在保护用户数据方面处于优势地位，其早在 2012 年就在 OSX Mountain Lion 中实施了控制措施，该框架被称为 "透明、同意和控制"，简称 TCC。从那时起，随着 macOS 的每次迭代，TCC 的范围不断扩大，未经过相关应用程序的控制时，用户几乎无法访问自己的数据或数据创建设备（比如摄像头和麦克风）。

已经有很多关于这对可用性的抱怨，但我们不打算在这里重新讨论这些。我们在本文中关注的是当用户和 IT 管理员期望 TCC 正常运作时，绕过 TCC 的多种方式。

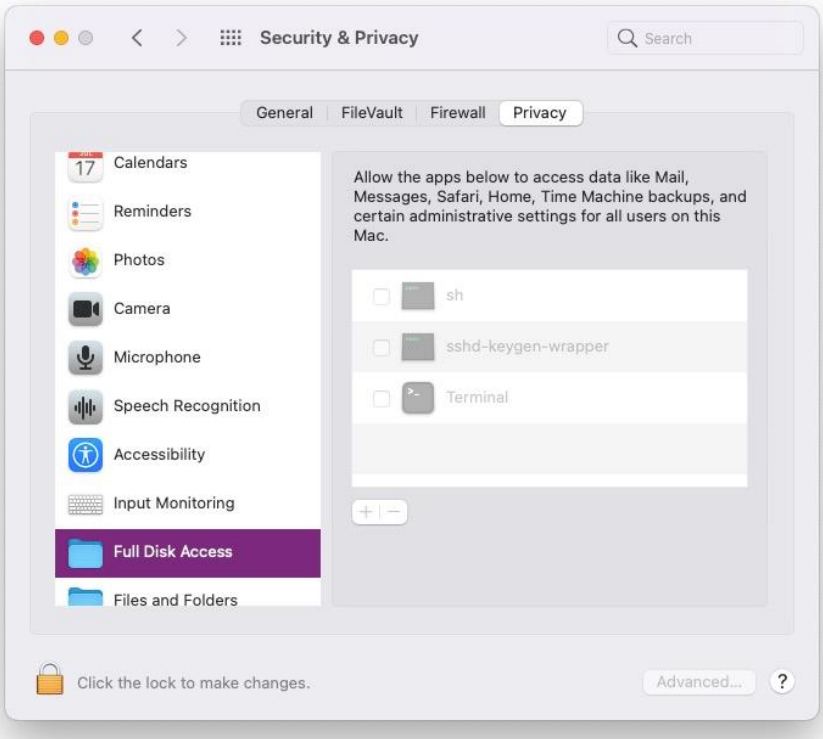
我们希望通过这些方式和问题，用户和管理员可以更好地了解敏感数据如何以及何时会被暴露，并希望他们在工作实践中考虑到这一点。

什么是 TCC

Apple 最新的平台安全指南不再提及 TCC 的名字，而是提到了 "保护应用程序对用户数据的访问"。Apple 在 5 月的平台安全指南中规定：

"Apple 设备利用各种技术帮助防止应用程序未经许可访问用户的个人信息……在 macOS 的系统偏好设置中，用户可以看到他们允许哪些应用程序访问某些信息，以及授予或撤销访问权限。"

通常情况下，我们谈论的隐私保护，主要由用户在“系统偏好设置“的”安全与隐私“窗格的“隐私”选项卡中进行管理。



System Preferences.app 提供了 TCC 的前端

由 MDM 解决方案控制的 Mac 设备也可以通过配置文件的方式设置各种隐私偏好。在实际情况下，这些偏好不会在上面的隐私窗格中被用户看到。但是，它们可以通过 TCC 数据库进行枚举。这样做的命令在 Big Sur 及之后的版本中略有变化。

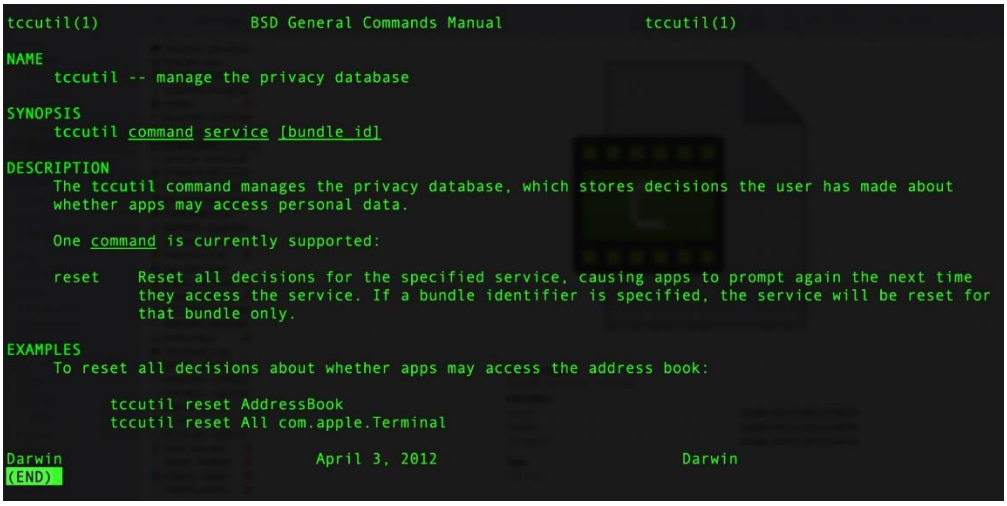
macOS 11 (Big Sur) 及更高版本：

```
sudo sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db " SELECT client ,auth_value FROM access WHERE service== 'kTCCServiceSystemPolicyAllFiles' " | grep '2'$
```

macOS 10.15 (Catalina) 及更早版本：

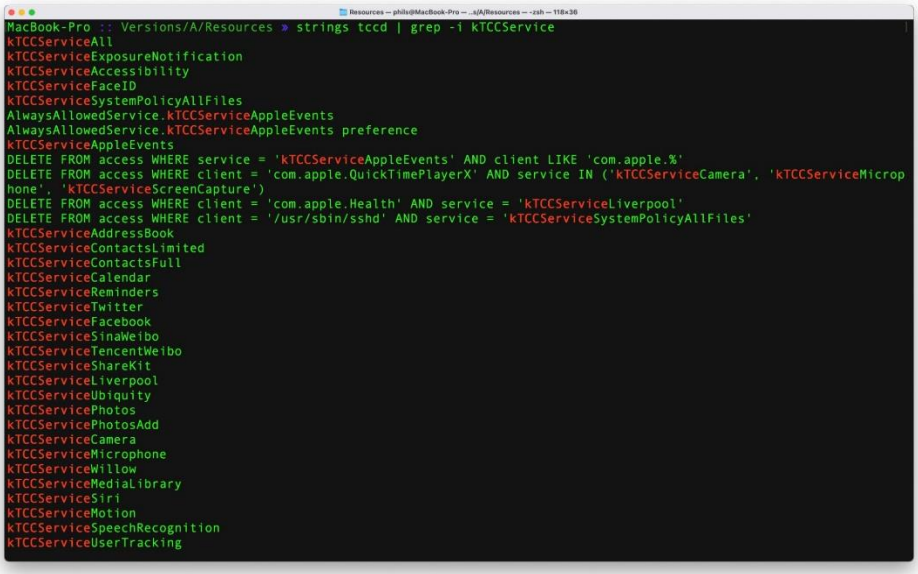
```
sudo sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db " SELECT client , allowed FROM access WHERE service == 'kTCCServiceSystemPolicyAllFiles' " | grep '1'$
```

命令行还为用户和管理员提供了/usr/bin/tccutil 工具，虽然它声称提供 "管理隐私数据库 "的能力有点夸大其词，因为它唯一记录的命令是 reset，但如果你需要清空系统或用户的 TCC 权限，这个工具还是很有用的，而其他方面就没什么用了。



tccutil 的 spartan man 页

在后台，这些权限都由位于 /System/Library/PrivateFrameworks/TCC.framework/Versions/A/Resources/tccd 的 TCC.framework 管理。



tccd 二进制文件中的字符串显示了一些提供 TCC 保护的服务

从一个相当狭隘的角度看待用户在实践中如何使用他们的 Mac，人们可以说，当用户（和应用程序）的行为符合预期时，Apple 公司用这个框架设计的隐私控制就会发挥作用。但正如我们现在将要看到的，当一个或两个都脱离脚本时就会出现问题。

全盘访问：一个打破所有规则的规则

要理解 Apple 公司在实现 TCC 中存在的问题，重要的是要了解 TCC 权限存在于两个层面：用户层面和系统层面。在用户层面，单个用户可以允许某些权限，这些权限被设计为只适用于他们自己的账户，而不是其他人。如果 Alice 允许终端访问她的桌面或下载文件夹，这对 Bob 来说不是什么难事。当 Bob 登录时，终端将不能访问 Bob 的桌面或下载文件夹。

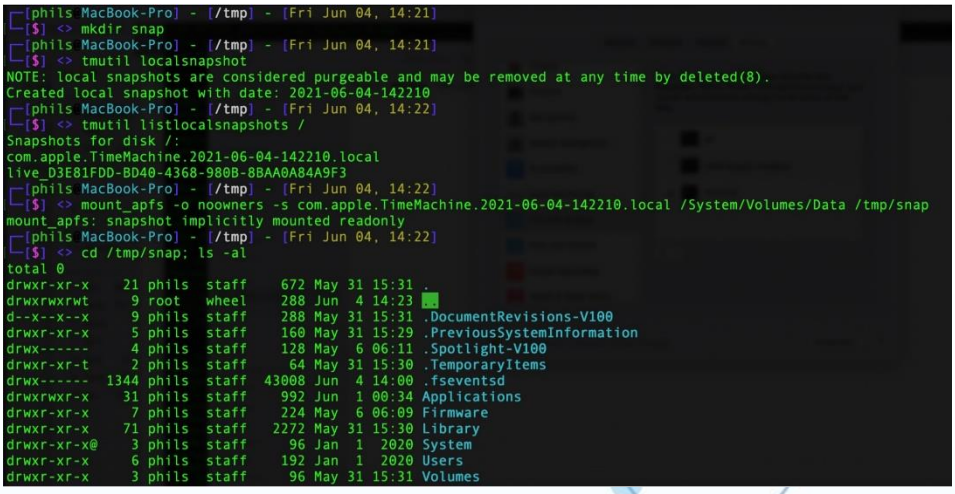
至少，它应该是这样工作的，但是如果 Alice 是一个管理员用户，并且给了终端全盘访问权（FDA），那么 Alice 可以很高兴地浏览 Bob 的桌面和下载文件夹（以及其他人的），

不管 Bob（或其他用户）设置了什么 TCC。请注意，如果 Bob 也是一个管理员用户，他不会得到任何特殊保护。全盘访问的意思是：它可以由一个具有管理员权限的用户来设置，并授予对全系统所有用户的数据的访问。

虽然这对系统管理员来说似乎是个好消息，但其中有一些含义可能不是很明显，它们会影响到管理员自己的数据安全。

当 Alice 为自己授予终端的 FDA 权限时，所有用户现在也通过终端拥有 FDA 权限。其结果是，Alice 不仅授予自己访问他人数据的特权，她也授予他人访问她的数据的特权。

令人惊讶的是，Alice 无意识放任的许可权也延伸到了非特权用户。正如 CVE-2020-9771 所报告的那样，允许终端拥有全盘访问权使所有的数据都可以被读取，没有任何进一步的安全挑战：整个磁盘可以被挂载，甚至被非管理员用户读取。具体的工作原理在 THEEVILBIT BLOG 的博客中有详细的阐述，简而言之，任何用户都可以创建并挂载系统的本地快照，并读取所有其他用户的数据。



即使是标准用户也可以读取管理员的私人数据

解决这个问题的"诀窍 "在于两个命令行工具，这两个工具对所有用户都可用，即 /usr/bin/tmutil 和/sbin/mount。第一个工具允许我们创建整个系统的本地快照，第二个

工具将快照挂载为 apfs 只读文件系统。从那里，我们可以浏览挂载的快照上捕获的所有用户数据。

重要的是要理解这不是一个 bug，也不会被修复（撰写本文时，Apple 的立场是"按预期工作"）。上面提到的 CVE 是能够在没有全盘访问的情况下利用这个错误，而 Apple 的修复方法是仅在授予全盘访问权限时才可能实现。对 Mac 管理员来说就是：

当你授予自己全盘访问权时，你就授予了所有用户（甚至是无特权的用户）读取磁盘上所有其他用户数据的能力，包括你自己的。

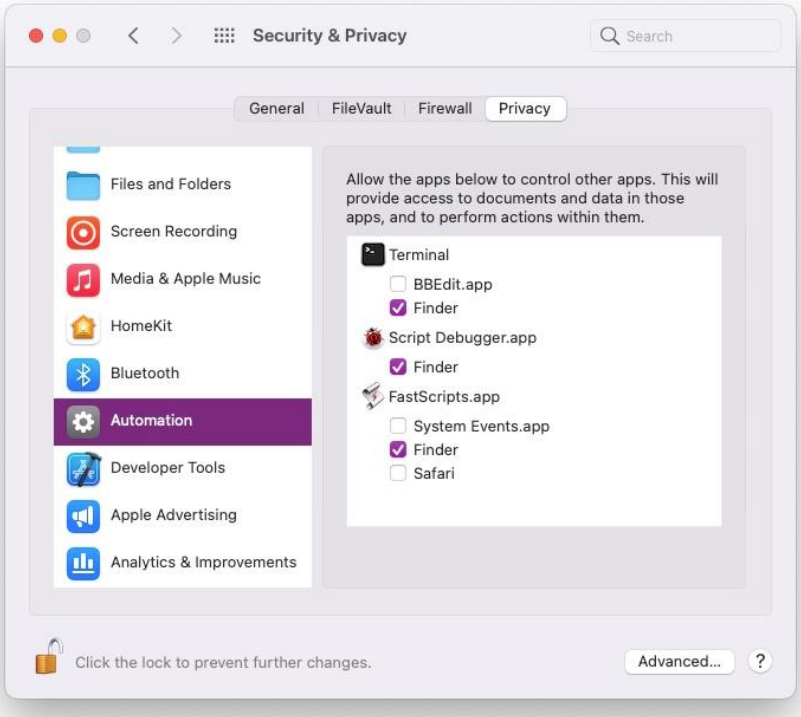
通过 Automation 后门全盘访问

这种情况不仅限于用户，它也延伸到了用户进程。根据设计，任何被授予全盘访问权的应用程序都可以访问所有用户数据。如果该应用程序是恶意软件，或者可以被恶意软件控制，那么恶意软件也可以。但是，应用程序的控制是由另一个 TCC 偏好管理的，即 Automation（自动化）。

这里还有一个陷阱：Mac 上有一个应用程序始终拥有全盘访问权，但从未出现在系统偏好设置中的全盘访问窗格中：Finder。

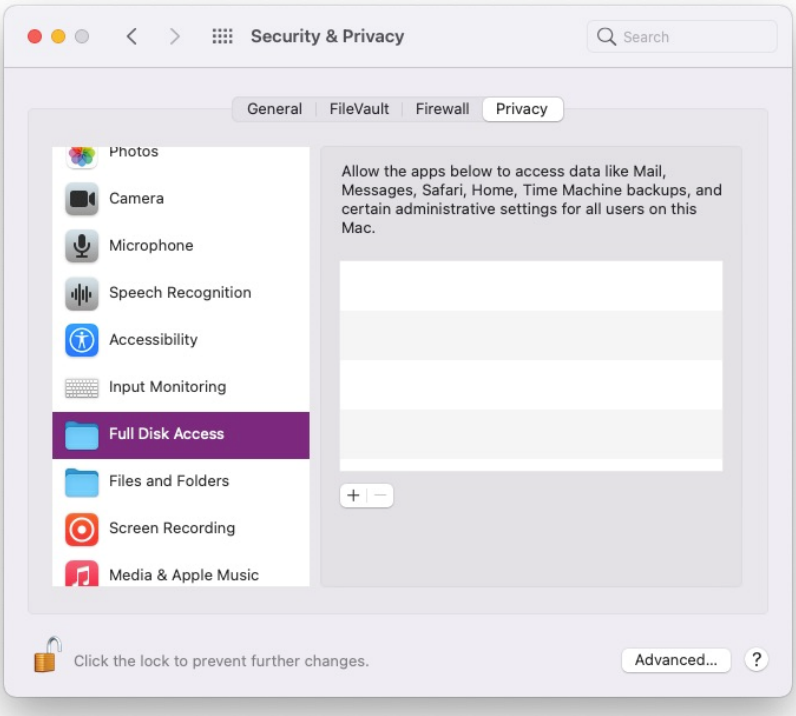
任何可以控制 Finder 的应用程序（在"隐私"窗格的 "Automation "中列出）也有全盘访问权，虽然你不会看到 Finder 或控制应用程序在全盘访问窗格中列出。

由于这种复杂性，管理员必须意识到，即使他们从未授予 FDA 权限，或者即使他们锁定了全盘访问权（也许是通过 MDM 解决方案），只要允许应用程序在 " Automation"窗格中控制 Finder，就会绕过这些限制。



Automation Finder 允许应用程序全盘访问

在上图中，Terminal 和两个合法的第三方 Automation 应用程序 Script Debugger 和 FastScripts 都具有全盘访问权 (通过 Finder)，虽然它们在全盘访问隐私窗格中没有显示。



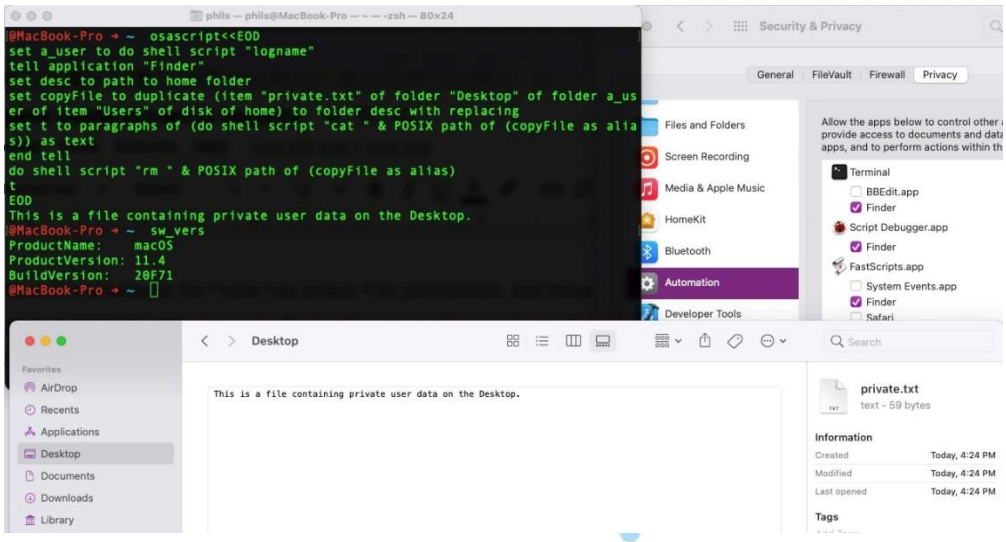
Automation FDA 后门的应用程序不显示在 FDA 窗格中

如上所述，这是因为 Finder 具有不可撤销的 FDA 权限，并且这些应用程序已经被赋予了对 Finder 的 Automation 控制。要了解这是如何工作的，这里有一个小演示：

```
~ osascript<<EOD
set a_user to do shell script "logname"
tell application "Finder"
set desc to path to home folder
set copyFile to duplicate (item "private.txt" of folder "Desktop" of folder a_user of item "Users" of disk of home) to folder desc with replacing
set t to paragraphs of (do shell script "cat " & POSIX path of (copyFile as alias)) as text
```

```
end tell

do shell script "rm " & POSIX path of (copyFile as alias)

t

EOD
```

虽然 Terminal 没有被授予全盘访问权，但如果它在过去由于任何原因被授予了 Automation 权限，在终端中执行上述脚本将返回 "private.txt "文件的内容。由于 "private.txt "位于用户的桌面上，一个表面上受 TCC 保护的位置，用户可能会合理地期望，如果没有应用程序被明确授予 FDA 权限，这个文件的内容将保持私有，但事实显然不是这样的。



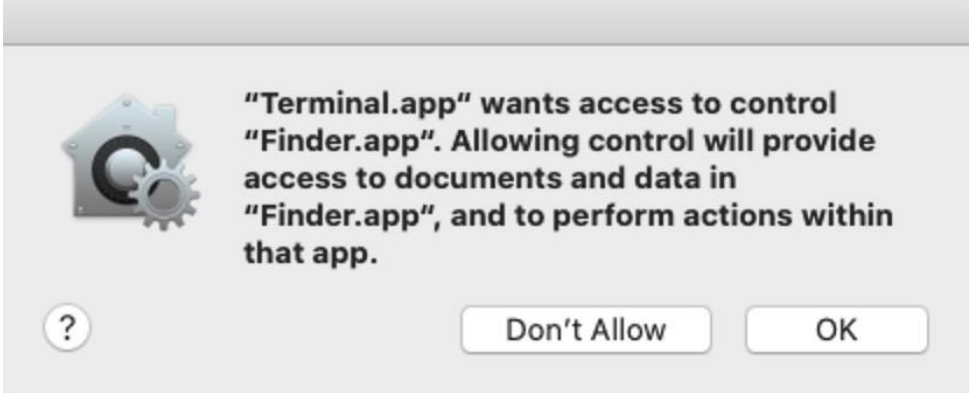
通过 Automation Finder 对 FDA 进行后门

很明显，这个问题的缓解措施是不允许应用程序自动执行 Finder。但是，我们注意有关该建议的两个要点：

首先，将 Finder 的 automation 授予终端或其它应用程序有许多合法的理由：任何对通过 automation 提高效率感兴趣的熟练的用户很可能已经这样做了，或正希望这样做。不

幸的是，这是一个 " All-In"的交易，如果用户有这样做的特定目的，则无法阻止终端（或其他程序）利用此权限执行的不合法操作。

第二，以这种方式对 FDA 进行后门访问会导致授权障碍的降低。以通常的方式授予 FDA 需要管理员密码。但是，人们可以在没有密码的情况下同意 Finder（以及 FDA 后门）的 automation，只需点击同意对话框就足够了：



一个简单的 "OK "就可以控制 Finder，并扩展到全盘访问。

虽然警告文本足够明确（如果用户阅读了它），但它远远不够透明，鉴于 Finder 不可撤销的全盘访问权，控制应用程序的权力远远超过了当前用户的同意或控制。

如果它曾经在过去的任何时候被授予过这种权限，那么这个权限仍然有效（因此对用户来说是透明的，但并不是好的），除非在系统偏好设置的 " automation "窗格中或通过前面提到的 tccutil reset 命令撤销。

总而言之：密切关注 "系统偏好 "的 "隐私"窗格中允许自动执行的内容。

TCC 绕过

到目前为止，我们提到的所有问题实际上都是设计导致的，但除此之外也要记住 TCC

绕过的漫长历史。当 macOS Mojave 首次公开发布时，SentinelOne 第一个注意到 TCC 可以通过 SSH 绕过。此后多个研究人员的研究表明，还有很多绕过的方法。

最近的 TCC 绕过是在 2020 年 8 月被 XCSSET 恶意软件利用之后曝光的。虽然 Apple 在大约 9 个月后的 2021 年 5 月修复了这个特殊的漏洞，但在未更新到 macOS 11.4 或最新的 10.15.7 的系统上，它仍然可以被利用。

在易受攻击的系统上，它很容易复现：

1.创建一个需要 TCC 权限的简单木马应用程序。在这里，我们将创建一个需要访问当前用户桌面的应用程序以枚举保存在那里的文件。

```
% osacompile -e 'do shell script "ls -al /Users/sphil/Desktop >> /tmp/lsout"' -o /tmp/ls.app
```

2. 将这个新的"ls.app"木马复制到一个已经获得 TCC 访问桌面权限的应用程序包中。

```
% cp -R /tmp/ls.app /Applications/Some\ Privileged.app/
```

可以通过"系统偏好设置"的"安全与隐私"面板的"隐私"选项卡中的"文件和文件夹"类别找到当前允许的应用程序列表（恶意软件采用另一种方式，我们将在稍后解释）。

3.执行木马应用程序：

```
% open /Applications/Some\ Privileged.app/ls.app
```

有安全意识的读者无疑会想，攻击者如何在不了解 TCC 权限的情况下实现第 2 步，因为无法从终端枚举 TCC.db 中的特权应用程序列表，除非终端已经拥有全盘访问权。

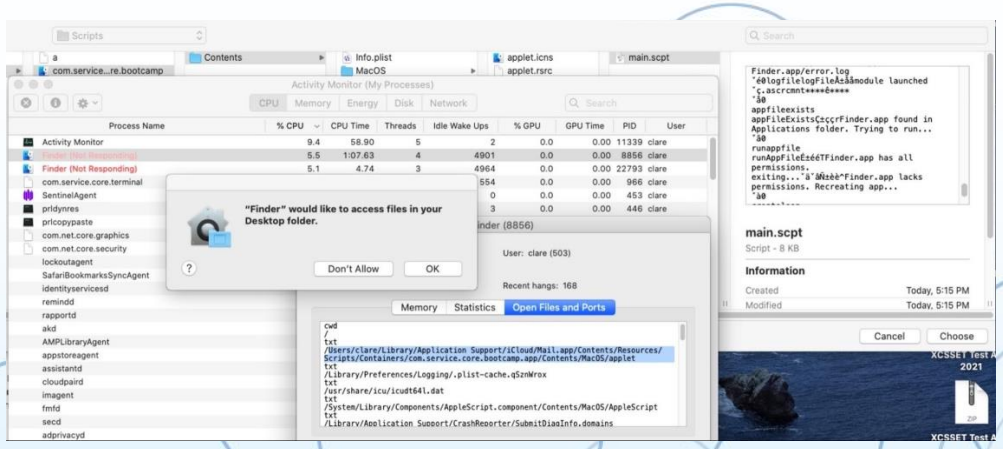
假设目标没有因为其他合法原因授予终端 FDA 权限，攻击者、红队成员或恶意软件可以列举/Applications 文件夹的内容，并根据内容进行有根据的猜测，如果在那里找到例如 Xcode、Camtasia 和 Zoom，这些应用程序如果安装，可能会获得特权。

同样，可以对已知具有此类权限的应用程序列表进行硬编码，并在目标机器上搜索它们。这正是 XCSSET 恶意软件的工作方式：该恶意软件硬编码了一个它期望拥有屏幕捕捉权限的应用程序列表，并将其自己的应用程序注入所发现的任何应用程序的捆绑包中。

```
00033 PushLiteral 9 #  ;  String: 'us.zoom.xos'

00034 PushLiteral 10 #  ;  String: 'com.hnc.Discord'

00035 PushLiteral 11 #  ;  String: 'WhatsApp'

00036 PushLiteral 12 #  ;  String: 'com.tinyspeck.slackmacgap'

00037 PushLiteral 13 #  ;  String: 'com.tencent.xinWeChat'

00038 PushLiteral 14 #  ;  String: 'com.teamviewer.TeamViewer'

00039 PushLiteral 15 #  ;  String: 'com.upwork.Upwork'

0003a PushLiteralExtended 16 #  ;  String: 'com.parallels.desktop.console'

0003d PushLiteralExtended 17 #  ;  String: 'com.parallels.desktop.appstore'

00040 PushLiteralExtended 18 #  ;  String: 'com.screenshotmonitor.SSM-App'

00043 PushLiteralExtended 19 #  ;  String: 'com.bohemiancoding.sketch3'

00046 PushLiteralExtended 20 #  ;  String: 'com.skype.skype'
00049 PushLiteralExtended 21 # <Value type=fixnum value=0xc>   ;  Decimal value = 12
```

XCSSET 恶意软件的解码字符串显示了它利用 TCC 权限的应用程序列表

不幸的是，对这个特殊漏洞的修复并不能有效阻止恶意软件开发者。如果绕过失败，只需冒充 Finder，向用户要求控制权，这是一个简单的问题。与 automation 请求一样，这只需要用户点击同意，而不是提供一个密码。

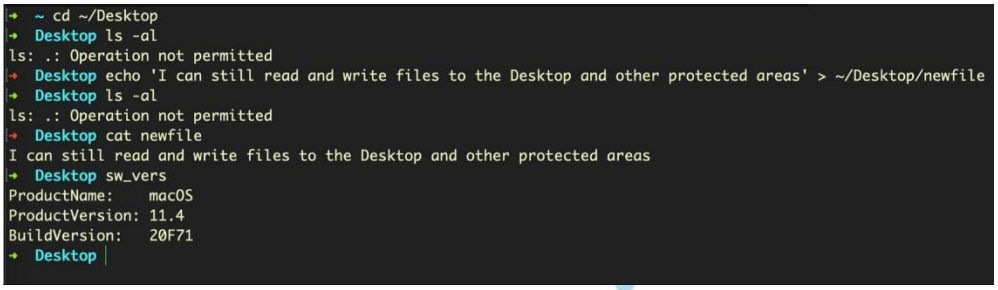


正如我们在上面指出的，Finder 已经默认拥有全盘访问权，所以用户看到要求授予 Finder 访问任何文件夹的请求对话框，应该立即警惕。

TCC 其它缺陷

关于我们对 TCC 问题的研究，除了上述内容，但还有一个值得注意的地方。通常对 Apple 用户隐私控制的一个常见误解是，它会阻止对某些位置的访问（例如桌面、文档、下载、iCloud 文件夹），但事实上并不完全如此。

管理员需要注意的是，TCC 并不能防止非特权进程将文件写入 TCC 保护区域，同样也不能阻止这些进程读取如此写入的文件。



进程可以写入 TCC 保护区，并读取它写入的文件

这很重要，因为如果用户安装了任何一种不能访问 TCC 保护区域的安全软件或监控软件，则没有什么可以阻止恶意软件将其部分组件或全部组件隐藏在这些保护区中。TCC 不会阻止恶意软件使用这些位置，这并不是每个 Mac 系统管理员都知道的盲点，所以不要依赖 TCC 来提供某种内置的受保护的 "安全区"。

结论

我们已经看到了 macOS 用户（尤其是管理员）如何在不知情的情况下，就轻易地暴露了他们认为受到 TCC 保护的数据。更让人讶异是，这些 "无心之失 "大多只是因为 TCC 自身缺乏透明度。比如，为什么 Finder 没有被列出在全盘访问窗格中？为什么没有意识到 Finder 的自动化（automation）是全盘访问的后门？还有，为什么密码认证被降级为一个简单的同意询问，而实际上却会被授予相同的特权？

这篇文章提出的其他问题涉及同意是否应该有更细粒度的控制，以便可以在特定时间间隔选择性地重复提示，以及（也许是最重要的）用户能否通过退出同一设备上其他用户授予的 FDA 来保护自己的数据。

我们知道，恶意软件滥用了其中的一些漏洞，而且还存在各种未修复的 TCC 漏洞。在这一点上，我们唯一的结论是，用户和管理员都不应该过于依赖和信任 TCC 的能力，因为它目前的实现是为了保护数据不受未经授权的访问。

原文链接：

https://labs.sentinelone.com/bypassing-macos-tcc-user-privacy-protections-by-accident-and-design/