2017 年 10 月 31 日，星期二

漏洞聚焦：Circle with Disney 中的多个漏洞

一般信息

思科 Talos 披露在 Circle with Disney 中发现的几个漏洞。Circle with Disney 是一种网络设备，用于监控孩子们在特定网络上的互联网使用情况。Circle 通过无线方式与您的家庭 Wi-Fi 配对，使您能够管理网络中的所有设备，包括平板电脑、电视或笔记本电脑。初始配对完成后，它还可以通过以太网进行配对。利用 iOS 或 Android 应用，家庭可为每个家庭成员创建独特的配置文件，从而帮助为每个人打造不同的在线体验。

从开始发现漏洞到对外发布消息，Circle Media 的安全团队一直都积极配合，堪称典范。他们迅速做出了响应并保持开放的沟通姿态。此外，Circle with Disney 还进行了专门设计，确保只要有软件更新，它就会将其推送到客户设备上。已收到这些更新的客户将会免于遭受这些漏洞的攻击。

恶意攻击者可以通过利用这些漏洞，获得各种访问和权限级别，包括更改网络流量、执行任意远程代码、注入命令、安装未签名的固件、接受非预期证书、绕过身份验证、升级权限、重启设备、安装永久性后门、覆盖文件，甚至将设备完全变成无用的砖块。

详情

TALOS-2017-0370 -- CVE-2017-2864

Circle with Disney 的身份验证令牌生成功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包，使系统向其返回有效的身份验证令牌，从而绕过身份验证。攻击者可以发送一系列数据包来触发此漏洞。

TALOS-2017-0371 -- CVE-2017-2865

Circle with Disney 的固件更新功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包，使产品运行攻击者所提供的 shell 脚本。攻击者可以拦截并更改网络流量来触发此漏洞。

TALOS-2017-0372 -- CVE-2017-2866

Circle with Disney 的 /api/CONFIG/backup 功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包注入 os 命令。攻击者可以发送 http 请求来触发此漏洞。

TALOS-2017-0388 -- CVE-2017-2881

Circle with Disney 的 torlist 更新功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包，使产品运行攻击者所提供的 shell 脚本。攻击者可以拦截并更改网络流量来触发此漏洞。

TALOS-2017-0389 -- CVE-2017-2882

Circle with Disney 的服务器更新功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包，使设备覆盖敏感文件，进而执行代码。攻击者需要假冒一个远程服务器，以触发此漏洞。

TALOS-2017-0390 -- CVE-2017-2883

Circle with Disney 的数据库更新功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包，使设备执行任意代码。攻击者需要假冒一个远程服务器，以触发此漏洞。

TALOS-2017-0391 -- CVE-2017-2884

Circle with Disney 的用户照片更新功能中存在一个可利用的漏洞。攻击者可以使用一组经特殊设计的重复的 API 调用导致设备的重要内存受损，进而让设备变成无用的砖块。攻击者需要通过网络连接到设备，以触发此漏洞。

TALOS-2017-0396 -- CVE-2017-2889

Circle with Disney 的 API 后台守护程序中存在一个可利用的拒绝服务漏洞。攻击者可以利用此漏洞发起大量并发 TCP 连接，导致 APID 后台守护程序重复分叉，进而让后台守护程序耗尽内存并触发设备重新启动。攻击者需要通过网络连接到设备，以触发此漏洞。

TALOS-2017-0397 -- CVE-2017-2890

Circle with Disney 的 /api/CONFIG/restore 功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包注入 os 命令。攻击者可以通过发送 HTTP 请求来触发此漏洞。

TALOS-2017-0405 -- CVE-2017-2898

Circle with Disney 的固件更新功能的签名验证中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包，在设备中安装未签名的固件，使设备执行任意代码。攻击者可以发送一系列数据包来触发此漏洞。

TALOS-2017-0418 -- CVE-2017-2911

Circle with Disney 的远程控制功能中的 rclient SSL 验证中存在一个可利用的漏洞。针对特定域名的证书会导致产品接受非预期的证书。攻击者可以使用此证书托管 HTTPS 服务器，触发此漏洞。

TALOS-2017-0419 -- CVE-2017-2912

Circle with Disney 的远程控制功能中的 goclient SSL 验证功能中存在一个可利用的漏洞。针对特定域名的 SSL 证书会导致产品接受非预期的证书。攻击者可以使用此证书托管 HTTPS 服务器，触发此漏洞。

TALOS-2017-0420 -- CVE-2017-2913

Circle with Disney 的远程控制功能中的 libbluecoat.so SSL 验证中存在一个可利用的漏洞。针对特定域名的 SSL 证书会导致产品接受非预期的证书。攻击者可以使用此证书托管 HTTPS 服务器，触发此漏洞。

TALOS-2017-0421 -- CVE-2017-2914

运行固件 2.0.1 的 Circle with Disney 的 API 后台守护程序中存在一个漏洞，攻击者可利用该漏洞绕过身份验证。攻击者可以使用经特殊设计的令牌绕过 Apid 二进制文件的身份验证例程，使设备授予非预期的管理访问权限。攻击者需要通过网络连接到设备，以触发此漏洞。

TALOS-2017-0422 -- CVE-2017-2915

Circle with Disney 的 WiFi 配置功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的 SSID，使设备执行长度受限的 shell 命令，从而执行代码。攻击者需要发送几个 HTTP 请求并设置设备可访问的无线接入点，以触发此漏洞。

TALOS-2017-0423 -- CVE-2017-2916

Circle with Disney 的 /api/CONFIG/restore 功能中存在一个可利用的漏洞。攻击者可使用经特殊设计的网络数据包，使设备覆盖任意文件。攻击者可以通过发送 HTTP 请求来触发此漏洞。

TALOS-2017-0424 -- CVE-2017-2917

Circle with Disney 的通知功能中存在一个可利用的漏洞。攻击者可以使用经特殊设计的网络数据包注入 os 命令。攻击者可以通过发送 HTTP 请求来触发此漏洞。

TALOS-2017-0435 -- CVE-2017-12083

Circle with Disney 的 Apid 后台守护程序中存在一个可利用的信息泄露漏洞。攻击者可以使用一组经特殊设计的数据包，使 Disney Circle 将字符串从内部数据库转储到 HTTP 响应中。攻击者需要通过互联网网络连接触发此漏洞。

TALOS-2017-0436 -- CVE-2017-12084

Circle with Disney 的远程控制功能中存在一个后门漏洞。攻击者可以使用一组经特殊设计的网络数据包远程启动设备上的 SSH 服务器，从而导致持久性后门。攻击者可发送 API 调用以启动 SSH 服务器。

TALOS-2017-0437 -- CVE-2017-12085

Circle with Disney 的云基础设施中存在于一个可利用的路由漏洞。攻击者可以使用经特殊设计的数据包，使 Circle 云将数据包路由到任意 Circle 设备上。攻击者需要通过互联网网络连接触发此漏洞。

TALOS-2017-0439 -- CVE-2017-12087

Circle with Disney 的 mdnsd 后台守护程序中存在一个可利用的堆溢出漏洞。攻击者可以使用经特殊设计的数据包，使 Circle 用攻击者控制的值来覆盖堆上任意数量的数据。攻击者需要通过网络连接到 Circle，以触发此漏洞。

TALOS-2017-0446 -- CVE-2017-12094

Circle with Disney 的 WiFi 信道分析中存在一个可利用的漏洞。攻击者可以使用经特殊设计的 SSID，让设备执行长度受限的 sed 命令。攻击者需要设置一个设备可访问的无线接入点，以触发此漏洞。

TALOS-2017-0448 -- CVE-2017-12096

Circle with Disney 的 WiFi 管理功能中存在一个可利用的漏洞。即使安全选项发生更改，Circle 设备也始终会连接到已配置的无线接入点 SSID。攻击者需要设置设备可访问的无线接入点并发送一系列欺骗性的“deauth”数据包来触发此漏洞。

防护

以下 Snort 规则可以检测此漏洞的漏洞攻击活动。请注意，Talos 将来可能会发布更多规则，当前规则会根据将来得到的更多漏洞信息而有所变更。有关最新的规则信息，请参阅您的 FireSIGHT 管理中心或 Snort.org

规则

43487-43488、43712、43714-43716、43861、43864、44012、44070、44082、44142、44162、44189、44267-44268、44297

发布者：WILLIAM LARGENT；发布时间：15:04

标签：零日攻击、CIRCLE WITH DISNEY、TALOS、漏洞聚焦