Apple多个最新在野0day漏洞通告

发布时间：2021-05-08 15:00:21

0x01 漏洞简述

近期360安全大脑在全网范围内侦测到多起针对Apple产品的高级威胁攻击，影响最新的iOS、macOS系统，最新的iPhone手机和苹果电脑无法防御相关攻击。360高级威胁研究院在确定漏洞的严重性后，第一时间将相关漏洞细节通知了苹果公司，苹果公司已于4月26日开始至5月陆续发布安全补丁修复相关0day漏洞，并安全公告致谢360安全团队。

通过该漏洞攻击者可以精心制作多个恶意网站诱导受害用户访问，恶意网页会判断受害者访问使用的浏览器类型，如果是Safari则发送携带exploit的JS代码，尝试多个浏览器漏洞和内核提权漏洞组合攻击，最终使用自定义的Loader加载一个Mash-o后门程序，攻击流程如下图。

后门程序主要功能：

1. 收集APP安装信息

2. 窃取通讯录中所有联系人信息

3. 窃取设备的UDID和设备序列号

4. 窃取IOS KeyChain中保存的应用账户密码信息

鉴于相关漏洞的严重危害，请Apple产品用户及时更新安全补丁。

0x02 风险等级

360CERT对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT评分	9.8

0x03 漏洞详情

CVE-2021-30666: Webkit缓冲区溢出漏洞

CVE: CVE-2021-30666

组件: iOS、macOS

漏洞类型: 缓冲区溢出

影响: 代码执行

简述: 处理恶意制作的Web内容可能会导致任意代码执行，该漏洞已有在野利用。

CVE-2021-30665: Webkit内存破坏漏洞

CVE: CVE-2021-30665

组件: iOS、macOS

漏洞类型: 内存破坏

影响: 内存破坏、代码执行

简述: 处理恶意制作的Web内容可能会导致任意代码执行，该漏洞已有在野利用。

CVE-2021-30661: Webkit内存释放重用漏洞

CVE: CVE-2021-30661

组件: iOS、macOS

漏洞类型: 内存释放重用

影响: 代码执行

简述: 处理恶意制作的Web内容可能会导致任意代码执行，该漏洞已有在野利用。

0x04 修复建议

通用修补建议

将系统更新至最新版本：

Apple官方更新教程

0x05 产品侧解决方案

360安全分析响应平台

360安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn)获取对应产品。

360本地安全大脑

360本地安全大脑是将360云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

0x06 时间线

2021-05-03 Apple官方发布安全更新

2021-05-08 360CERT发布通告

0x07 参考链接

1、 HT212341

2、 HT212336

0x08 特制报告下载链接

一直以来，360CERT对全球重要网络安全事件进行快速通报、应急响应。为更好地为政企用户提供最新漏洞以及信息安全事件的安全通告服务，现360CERT正式推出安全通告特制版报告，以便用户做资料留存、传阅研究与查询验证。 用户可直接通过以下链接进行特制报告的下载。

Apple多个最新在野0day漏洞通告

若有订阅意向与定制需求请发送邮件至 g-cert-report#360.cn ， 并附上您的 公司名、姓名、手机号、地区、邮箱地址。

漏洞预警

发表评论

发表你的评论吧

发表评论

评论列表

加载更多