安全漏洞通告

Apple 多个最新在野 0day 漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-05-08

报告信息

报告名称	Apple 多个最新在野 0day 漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-050801
报告版本	1	**报告日期**	2021-05-08
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-05-08	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	缓冲区或栈溢出
CVE 编号	CVE-2021-30666 等
相关厂商	apple
相关组件	ios、macos
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案
漏洞发布时间	2021-05-08
报告生成时间	2021-05-08

二、 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。

三、 漏洞评级

经过安全技术人员的分析，最终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

四、 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。

五、 影响版本

产品名称	影响版本
Apple:iOS、macOS	

六、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-30666	缓冲区或栈溢出		严重
CVE-2021-30665	内存破坏	内存破坏	严重
CVE-2021-30661	内存释放重用	内存释放重用	严重

七、 安全建议

(一) 通用修补方案

将系统更新至最新版本:

[Apple 官方更新教程](https://support.apple.com/zh-cn/HT201222)

八、 产品侧解决方案

(一) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。

(二) 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。

(三) 360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。

(四) 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。

九、 参考链接

1. HT212341

   https://support.apple.com/en-us/HT212341

2. HT212336

   https://support.apple.com/en-us/HT212336

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危