安全漏洞通告

Apple 任意代码执行漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	Apple 任意代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-072701
报告版本	1	报告日期	2021-07-27
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-07-27	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 27 日，360CERT 监测发现 Apple 发布了 macOS、iOS、iPadOS远程代码执行漏洞 的风险通告，漏洞编号为 CVE-2021-30807 ，漏洞等级：高危，漏洞评分：8.5。

macOS、iOS、iPadOS 是 Apple 公司的操作系统，在全球拥有庞大的用户基数。这些操作系统中的 IOMobileFrameBuffer 内核拓展中存在一处任意代码执行漏洞。攻击者可以通过诱使用用户打开特制的应用程序，即可以内核权限（最高权限）在用户设备上执行任意代码。

对此，360CERT 建议广大用户及时将 macOS、iOS、iPadOS 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

2 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	高危
影响面	广泛
攻击者价值	极高
利用难度	高
360CERT 评分	8.5

3 漏洞详情

3.1 CVE-2021-30807: macOS,iOS,iPadOS 代码执行漏洞

CVE: CVE-2021-30807

组件: macOS,iOS,iPadOS

漏洞类型: 代码执行

影响: 设备接管

简述: macOS、iOS、iPadOS 操作系统中的 IOMobileFrameBuffer 内核拓展中存在一处任意代码执行漏洞。攻击者可以通过诱使用用户打开特制的应用程序，即可以内核权限（最高权限）在用户设备上执行任意代码。

4 影响版本

组件	影响版本	安全版本
Apple:iOS	14.7.1	14.7.1（版本内修复）
Apple:iPadOS	14.7.1	14.7.1（版本内修复）
Apple:macOS	11.5.1	11.5.1 （版本内修复）

5 修复建议

5.1 通用修补建议

建议打开 Apple 设备的自动更新功能。本次安全更新已经可以通过自动更新下载安装

6 时间线

2021-07-26 Apple 发布通告

2021-07-27 360CERT 发布通告

7 参考链接

About the security content of macOS Big Sur 11.5.1

About the security content of iOS 14.7.1 and iPadOS 14.7.1

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 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。

A.2 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。