

快讯 | macOS漏洞导致本地管理员可以使用任何密码解锁App Store系统设置

 [Sphinx](#)  2018-01-12 共7967人围观，发现 1 个不明物体

系统安全



macOS 10.13.2系统中被爆出一个新漏洞，利用漏洞可以让本地管理员用任何用户名密码解锁App Store系统设置。就是说如果你在办公室里离开时没有锁屏，别人就可以更改你的App Store设置。



使用这个漏洞非常简单，只需要打开App Store系统设置，如果小锁被锁住，点击它，macOS会提示输入密码。输入



经过测试，漏洞在macOS 10.13.1版本上无效。另外macOS High Sierra 10.13.3的第三和第四个测试版也无效，因此漏洞可能只对10.13.2和10.13.3的早期beta版有效。

过去的3个月里这已经是macOS第二次被爆出于密码有关的漏洞了，上次的漏洞可以让用户不断地按回车键获取root权限。

macOS High Sierra能让用户创建一个空密码的root账号，攻击者通过反复按键就可以创建root账号，之后就可以登陆设备，root账号也可以被用来远程访问。

* 参考来源: [BleepingComputer](#)，作者Sphinx，转载注明来自Freebuf.COM

上一篇: [来自BlackHat的新姿势：Process Doppelganging攻击技术与贴身防护](#)

下一篇: [本篇已是最新文章](#)

已有 1 条评论

孙一峰 2018-01-12

1楼 [回](#)

最近MacOS越权漏洞有点多

 亮了 1

选择文件 未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。 [登陆?](#) [注册](#)

邮箱

请输入邮箱地址

必须 (保密)

表情

插图

提交评论(Ctrl+Enter)

[取消](#)



有人回复时邮件通知我

Sphinx

这家伙太懒了，什么都没写

317

文章数

70

评论数

最近文章

- 快讯 | macOS漏洞导致本地管理员可以使用任何密码解锁App Store系统设置
 - 旧版Windows打上CPU补丁后会出现性能下降
 - 2018年的安全市场，Gartner怎么看？
- 2018.01.12

2018.01.11

2018.01.09

浏览更多

相关阅读

[关于一个macOS 10.12.2到macOS 10.12...](#)

[macOS平台最新恶意软件HiddenLotus...](#)

[快讯 | MacOS重大漏洞：反复按键即可...](#)

[研究人员公开披露macOS 0-day漏洞详...](#)

[iPhone和Mac用户请注意：接收一条M...](#)

特别推荐






| | |
|---|---|
| 极客DX：手机文件直传U盘，三步教你做一根OTG传输线 <small>关注我们 分享每日精选文章</small> geekman 2014-12-27 | 独家分析：安卓“Janus”漏洞的产生原理及利用过程 顶象技术 2017-12-12 |
| 量子计算从概念走入现实，公钥加密是否岌岌可危 Elaine_z 2017-07-18 | 快讯：联想官网被黑，内部邮件被劫持 hujias 2015-02-26 |



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务



