安全事件通告

Homebrew cask 恶意软件包投毒威胁通告

360CERT
北京奇虎科技有限公司 | 2021-04-22

报告信息

报告名称	Homebrew cask 恶意软件包投毒威胁通告		
报告类型	安全事件通告	**报告编号**	B6-2021-042201
报告版本	1	**报告日期**	2021-04-22
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	2021-04-22	360CERT	360CERT	撰写报告

目录

一、 事件档案

相关厂商	Homebrew
相关组件	Homebrew
威胁等级	严重
影响面	广泛
360CERT 评分	10.0
修复方案	通用修补方案
漏洞发布时间	2021-04-22
报告生成时间	2021-04-22

二、事件简述

2021 年 04 月 22 日，360CERT 监测发现 Homebrew 官方发布了安全事件通告，事件等级：严重，事件评分：10.0。

Homebrew 是一款自由及开放源代码的软件包管理系统，用以简化 macOS 系统上的软件安装过程，因其可扩展性得到了一致好评，而在 Ruby on Rails 社区广为人知。 Homebrew 使用 GitHub，通过用户的贡献扩大对软件包的支持。

2021 年 04 月 18 日，国外安全人员在 Homebrew 项目中发现其 review-cask-pr GitHub Action 存在缺陷，攻击者可以将任意代码注入到 cask 类型的软件包中，并将其合并到包管理库的主分支上。当用户使用 brew upgrade 安全装软件包更新时，会将恶意包下载并执行其中的恶意代码。

对此，360CERT 建议广大用户好资产自查以及预防工作，以免遭受黑客攻击。

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	10.0

四、 事件详情

Homebrew 组织使用 review-cask-pr Github Action 程序自动审核用户提交的软件包，并将其合并到 homebrew-cask 或 homebrew-cask-*仓库的主分支中。

在 review-cask-pr 中使用了 git_diff 依赖，当其解析用户提交的合并请求时会对合并进行 diff 检查，由于其 diff 检查逻辑存在缺陷，将忽略存在问题的代码，从而使存在恶意代码的合并请求通过验证完成自动合并。

五、 安全建议

(一) 通用修补方案

目前官方已经采取紧急措施:

- 存在漏洞的 review-cask-pr GitHub Action 已经被禁用，并从所有的仓库中移除。

- 自动合并的 GitHub Action 已经被禁用，并从所有的仓库中删除。

- 已经删除了自动提交到 Homebrew/cask*目录的功能。

在测试该漏洞期间官方已做无害化的处理，在此期间使用的用户不受任何影响。

目前暂无消息表明该漏洞在公布前存在在野利用。

360CERT 建议使用 homebrew 的用户及时排查 /usr/local/Homebrew/Library/Taps/homebrew/homebrew-*目录下的 ruby 文件中是否存在恶意代码，避免遭受黑客攻击。

六、 产品侧解决方案

(一) 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。

(二) 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。

七、 参考链接

1. Homebrew 官方威胁通告

   https://brew.sh/2021/04/21/security-incident-disclosure/

2. hackerone 针对该漏洞的讨论

   https://hackerone.com/reports/1167608

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