JSPatch 平台关于苹果警告的解决方案

2017-03-10 bang JSPatch

苹果近期给大部分接入 JSPatch 的 APP 发送了警告，提示下个版本去掉拥有动态修改功能的代码或框架。

我们理解苹果这个决定是为了杜绝 JSPatch 使用不当导致的安全隐患以及恶意滥用，在此建议大家在**下个版本先去除 JSPatch。**

热修复本身可以显著提升 App 质量，对于 iOS 平台是很有益的事情，鉴于热修复的需求量庞大，我们也在思考如何让热修复继续发挥作用提升 iOS 平台 APP 的质量，同时又可以解决这里面的安全和滥用的隐患。

对此后续 JSPatch 平台 (http://jspatch.com) 会有以下升级改进：

1.强制脚本下发必须使用自定义 RSA 私钥加密。

这个功能 JSPatch 平台一直提供，不过不是强制使用，默认会使用平台统一的 RSA 私钥加密，这里会有一定的安全隐患。强制用户使用自己生成的 RSA 私钥后，平台本身完全无权限给用户下发脚本，就算平台被第三方恶意入侵也不会对 APP 有任何影响，不可能出现大规模安全事件。

2.禁止 SDK 接入

SDK 接入 JSPatch 后有能力对所有接入该 SDK 的 APP 下发脚本，SDK 覆盖面大以后，这里也是一个安全隐患，平台会禁止 SDK 接入 。

3.检查每个下发的脚本，禁止调用私有 API，禁止下发大量代码。

这里是避免热修复被滥用，利用动态下发去做一些违反 Apple 规则的事情，同时让热修复只用于修复 bug，而不是试图改变整个 APP 的功能。

平台升级后，接入平台的 APP 不会再有任何安全隐患，同时也可以强制禁止滥用。

鉴于 React Native / weex / 小程序 等动态化方案仍被允许，相信苹果并不拒绝动态方案，只是无法接受平台上有任何安全隐患和绕过审核调私有 API 侵犯用户隐私的行为，平台升级后可以帮助苹果解决这些问题，甚至如果苹果愿意，我们可以开放后台让苹果主导审核程序。

建议平台用户在 APP 下个版本去掉原有的 JSPatch SDK，**在平台升级后再接入新的 SDK**，升级完成后我们会通知大家。

热修复可以显著提升 APP 的开发效率和质量，有庞大的需求量，希望可以共建良好的热修复环境。

阅读原文