敲敲打打：一系列云端输入法漏洞使网络攻击者得以监看个人用户的输入内容（摘要）

- 重要：我们建议所有用户立即更新所使用的输入法软件以及操作系统。并建议高风险用户停止使用任何输入法提供的云端建议功能，改为完全离线的输入法，以避免数据外泄。
- 本文是完整版报告的摘要翻译。

重要发现

- 我们分析了常见云端拼音输入法的安全性，包含百度、荣耀、华为、讯飞、OPPO、三星、腾讯等九家厂商，并分析了它们发送用户输入内容到云端的过程是否含有安全缺陷。
- 分析结果指出，九家厂商中，有八家输入法软件包含严重漏洞，使我们得以完整破解厂商设计用于保护用户输入内容的加密法。亦有部分厂商并未使用任何加密法保护用户输入内容。
- 综合本研究和我们先前研究中发现的搜狗输入法漏洞，我们估计至多有十亿用户受到这些漏洞影响。基于下述原因，我们认为用户输入的内容可能已经遭到大规模收集：
  - 这些漏洞影响了广泛的用户群体
  - 用户在键盘中输入的信息极为敏感
  - 发现这些漏洞不需要高深技术
  - 五眼联盟过去曾利用中国应用程序中类似的漏洞施行监控
- 我们已向受影响的九家开发商提交这些漏洞，大部分开发商均认真看待问题并予以回应，修补了漏洞，但仍有少数输入法未修补漏洞。
- 在报告的末尾，我们为受漏洞影响的各方提供了综合建议，期待这些建议可以减少未来类似漏洞所造成的危害。

漏洞总结

在我们测试的九家厂商的应用程序中，仅有华为的产品未发现任何上传用户输入内容至云端相关的安全问题，其余每一家厂商都至少有一个应用程序含有漏洞，使得被动型网络攻击者得以监看用户输入的完整内容。

注：主动型网络监听攻击意指监听时必须要主动发出讯号，例如在信息传输过程中篡改少数比特数据，才能破解加密内容。主动型网络监听相对容易被侦测到。被动型网络监听攻击意指无需发出任何讯号，单纯读取传输中的的数据，即可达成解密。与主动性攻击相比，被动型网络监听攻击难以被侦测到。

图例	✘✘	**主动和被动**型网络监听者均可以破解加密的用户输入内容，已被我们成功实测
	✘	**主动**型网络监听者可以破解加密的用户输入内容，已被我们成功实测
	!	加密法实操中存在弱点
	✔	未发现问题
	N/A	该产品在我们测试的设备上不提供或是不存在

输入法开发商	Android				iOS	Windows
腾讯†	✘				N/A	✘
百度	!				!	✘✘
讯飞	✘✘				✔	✔
	内置输入法开发商					
装置制造商	自有	搜狗	百度	讯飞		
三星	✘✘	✔*	✘✘	N/A	N/A	N/A
华为	✔*	✔	N/A	N/A	N/A	N/A
小米	N/A	✘*	✘✘	✘✘	N/A	N/A
OPPO	N/A	✘	✘✘*	N/A	N/A	N/A
Vivo	✔*	✘	N/A	N/A	N/A	N/A
荣耀	N/A	N/A	✘✘*	N/A	N/A	N/A

* 在我们的测试设备上，此为默认的输入法

† QQ 输入法及搜狗输入法都是由腾讯开发，本研究中我们分析了 QQ 输入法，发现它含有我们先前在搜狗输入法中发现的相同漏洞

补丁总结

我们依据漏洞披露政策，向各厂商提交了所发现的漏洞。除了百度、Vivo 和小米，其余厂商皆回复了我们。在我们提交这些漏洞不久之后，百度修复了当中最严重的几个，但并未修补其余漏洞。数家手机制造商在操作系统中内置了这些带有漏洞的输入法程序，除了百度输入法之外，如今手

机制造商都已对内置输入法的这些漏洞作出修补。针对内置的百度输入法，荣耀完全未修补任何漏洞，其余厂商都只修补了部分最严重的漏洞。我们与厂商的联络内容、时间以及其它细节，参见我们的完整版报告。

图例	✘✘	**主动和被动**型网络监听者均可以破解加密的用户输入内容，已被我们成功实测
	✘	**主动**型网络监听者可以破解加密的用户输入内容，已被我们成功实测
	!	加密法实操中存在弱点
	✔	未发现问题
	N/A	该产品在我们测试的设备上不提供或是不存在

输入法开发商	Android				iOS	Windows
腾讯†	✘				N/A	✘
百度	!				!	!
讯飞	✔				✔	✔
	内置输入法开发商					
装置制造商	自有	搜狗	百度	讯飞		
三星	✔	✔*	!	N/A	N/A	N/A
华为	✔*	✔	N/A	N/A	N/A	N/A
小米	N/A	✔*	!	✔	N/A	N/A
OPPO	N/A	✔	! *	N/A	N/A	N/A
Vivo	✔*	✔	N/A	N/A	N/A	N/A
荣耀	N/A	N/A	✘✘*	N/A	N/A	N/A

* 在我们的测试装置上，这个是默认的输入法

† QQ 输入法及搜狗输入法都是由腾讯开发，本研究中我们分析了 QQ 输入法，发现它含有我们先前在搜狗输入法中发现的相同漏洞

总结来说，除了荣耀以外，我们发现的加密破解方法在经过厂商修补后，均已无效。而在荣耀手机以外厂牌的百度输入法中，仍持续存在加密的弱点，但我们暂时还未找到方法可以利用这些弱点破解传输中的用户输入内容。

受影响的软件列表

我们建议所有用户将操作系统和应用程序（包含输入法）升级到最新版本，若您使用了下列软件，我们强烈建议您检查并安装这些软件及操作系统最新的补丁。截至 2024 年 4 月 1 日，下列软件已有可供安装的更新补丁，安装后可修补我们发现的安全漏洞。

非操作系统内置（手动安装）的第三方开发者的输入法：

- Android 和 Windows 平台的 Sogou IME / 搜狗输入法
- Android 和 Windows 平台的 Baidu IME / 百度输入法（此开发者未完整修补我们发现的漏洞，详情见下）
- Android 平台的 iFlyTek IME / 讯飞输入法

三星中国版操作系统中内置输入法：

- Samsung Keyboard
- Baidu IME / 百度输入法

小米中国版操作系统中内置输入法：

- Sogou IME Xiaomi Version / 搜狗输入法小米版
- iFlyTek IME Xiaomi Version / 讯飞输入法小米版

OPPO 中国版操作系统中内置输入法：

- Sogou IME Custom Version / 搜狗输入法定制版

Vivo 中国版操作系统中内置输入法：

- Sogou IME Custom Version / 搜狗输入法定制版

下列软件仍未使用 TLS 加密协议，因此可能仍有漏洞：

非操作系统内置（手动安装）的第三方开发者的输入法：

- Android, Windows, 和 iOS 平台的 Baidu IME / 百度输入法

小米中国版操作系统中内置输入法：

- Baidu IME Xiaomi Version / 百度输入法小米版

OPPO 中国版操作系统中内置输入法：

- Baidu IME Custom Version / 百度输入法定制版

下列软件含有未修补的漏洞，能够轻易被攻击者所利用，我们建议用户改用其它输入法：

非操作系统内置（手动安装）的第三方开发者的输入法：

- Android 和 Windows 平台的 QQ Pinyin IME / QQ 输入法

荣耀中国版操作系统中内置输入法：

- Baidu IME Honor Version / 百度输入法荣耀版

综合建议

致信息安全研究人员

- 信息安全研究人员应多加研究东亚及其它热门区域的移动应用程序生态系，哪怕这些区域并非研究人员的原生区域。
- 信息安全研究人员应进一步发展动态及静态分析方法，以利大规模寻找本研究发现的此类型漏洞。
- 信息安全研究人员通报程序漏洞时应以程序开发者所在地区的常见语言写出简短摘要及邮件标题。

致应用商店

- 应用商店不应要求必须注册帐号才能下载安全补丁。
- 应用商店不应以设备的地理位置为由阻挡安全补丁。
- 如同 Google Play 商店，其他应用商店应提供方式给开发者标示隐私和安全信息，包含网络数据传输是否加密。
- 当开发者在应用商店中标示应用程序会加密所有传输数据时，应用商店应予以显示，当开发者并未如此标示时，应用程序商店亦应警告用户。
- 应用商店应针对特定敏感类型的应用程序（例如输入法）要求开发者保证所有传输数据均经加密，或保证不上传任何数据。

致输入法开发者

- 使用经过广泛测试的标准加密通信协议，例如 TLS 及 QUIC。
- 尽可能将功能设计为可离线运作、不需上传任何敏感数据到云端服务器。

致移动操作系统开发者

- 如同 iOS, Android 应通过沙盒化来限制输入法程序的网络传输和其它危险行为，在用户主动允许前不予放行。
- Android 及 iOS 开发者应设计更好的「网络访问」权限，让用户一目了然应用程序是否通过网络传输任何数据。

致智能手机制造商

- 将输入法集成并内置在操作系统之前，应稽核其安全性。

致一般用户

- 搜狗、QQ、百度、讯飞输入法的用户，无论输入法是手动从应用商店安装或者原本就内置在操作系统当中，应确保输入法及操作系统维持在最新版本。
- 顾虑隐私的用户应停用任何输入法中的云端功能。
- 顾虑隐私的 iOS 用户不要启用输入法的「允许完整访问权」。