敲敲打打：一系列雲端輸入法漏洞允許網路攻擊者監看輸入內容（摘要）

- 重要：我們建議所有使用者立即更新他們所使用的輸入法軟體以及作業系統。並建議高風險使用者停止使用任何輸入法提供的雲端建議功能，改為使用完全離線的輸入法，以避免資料外洩。
- 本文是完整報告的摘要翻譯。

重要發現

- 我們分析了常見雲端拼音輸入鍵盤的安全性，包含百度、榮耀、華為、訊飛、OPPO、三星、騰訊九家廠商，並檢視了它們傳送使用者輸入到雲端的過程是否含有安全缺陷。
- 分析結果指出，九家廠商中，有八家輸入法軟體包含嚴重漏洞，讓我們得以完整破解廠商設計用於保護使用者輸入內容的加密法。亦有部分廠商並未使用任何加密法保護使用者輸入內容。
- 綜合本研究和我們先前研究中發現的搜狗輸入法漏洞，我們估計至多有十億使用者受到這些漏洞影響。基於下述原因，我們認為使用者輸入的內容可能已經遭到大規模收集：
  - 這些漏洞影響眾多使用者
  - 使用者在鍵盤中輸入的資訊極為敏感
  - 發現這些漏洞不需要高深技術
  - 五眼聯盟過去曾利用中國應用程式中類似的漏洞施行監控
- 我們已向受影響的九家開發商回報這些漏洞，大部分開發商均認真看待並回應我們，並修補漏洞，但仍有少數輸入法未修補漏洞。
- 在報告的最後，我們提供綜合建議予受漏洞影響的各方，我們期待這些建議可以減少未來類似漏洞所造成的危害。

漏洞總結

在我們測試的 9 家廠商的應用程式中，僅有華為的產品未被發現任何傳輸使用者輸入相關的安全問題，其餘每一家廠商都至少有一個應用程式含有漏洞，使得被動的網路攻擊者得以監看使用者輸入的完整內容。

註：主動的網路監聽意指監聽時必須要主動發出訊號，例如在傳輸過程中篡改少數資料位元，才能達成解密。主動的網路監聽有可能可以被偵測到。被動的網路監聽意指無需發出任何訊號，單純讀取傳輸中的的資料，即可達成解密。被動的網路監聽難以被偵測到。

圖例	✘✘	**主動和被動**的網路監聽者可以破解加密的使用者輸入內容，且我們成功實測此方法
	✘	**主動**的網路監聽者可以破解加密的使用者輸入內容，且我們成功實測此方法
	!	加密法實作中存在弱點
	✔	未發現問題
	N/A	該產品在我們測試的裝置上不提供或是不存在

輸入法開發商	Android				iOS	Windows
騰訊†	✘				N/A	✘
百度	!				!	✘✘
訊飛	✘✘				✔	✔
	預載輸入法開發商					
裝置製造商	自有	搜狗	百度	訊飛		
三星	✘✘	✔*	✘✘	N/A	N/A	N/A
華為	✔*	✔	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
榮耀	N/A	N/A	✘✘*	N/A	N/A	N/A

* 在我們的測試裝置上，這個是預設的輸入法

† QQ 輸入法及搜狗輸入法都是由騰訊所開發，本研究中我們分析了 QQ 輸入法，發現它含有我們先前在搜狗輸入法中發現的相同漏洞

修補總結

我們依據漏洞揭露政策，向各廠商回報了所發現的漏洞。除了百度、Vivo 和小米，其他廠商皆有回覆我們。在我們回報漏洞不久之後，百度修復了當中最嚴重的幾個，但並未修補其餘漏洞。數家手機製造商預載了有漏洞的輸入法程式，除了預載的百度輸入法之外，如今手機製造商都已經修補了這些漏洞。針對預載的百度輸入法，榮耀完全未修補任何漏洞，其餘廠商都只修補了部分

最嚴重的漏洞。關於 QQ 輸入法，騰訊早先表示（中譯）：「撤除已停止維護的產品，我們計劃將於 [2024] 第一季前將所有使用 EncryptWall （加密法）的活躍產品升級為使用 HTTPS。」截至 2024 年 4 月 1 日，我們未發現騰訊提供任何 QQ 輸入法的修補，儘管 QQ 輸入法仍提供外界下載，騰訊自 2020 年起就未再提供 QQ 輸入法的更新，可能已經將此產品視為停止維護。我們與廠商的聯絡內容、時間以及其他細節，請見我們的完整版報告。

圖例		
	✘✘	**主動和被動**的網路監聽者可以破解加密的使用者輸入內容，且我們成功實測此方法
	✘	**主動**的網路監聽者可以破解加密的使用者輸入內容，且我們成功實測此方法
	!	加密法實作中存在弱點
	✔	未發現問題
	N/A	該產品在我們測試的裝置上不提供或是不存在

輸入法開發商	Android				iOS	Windows
騰訊 †	✘				N/A	✘
百度	!				!	!
訊飛	✔				✔	✔
	預載輸入法開發商					
裝置製造商	自有	搜狗	百度	訊飛		
三星	✔	✔*	!	N/A	N/A	N/A
華為	✔*	✔	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
榮耀	N/A	N/A	✘✘*	N/A	N/A	N/A

* 在我們的測試裝置上，這個是預設的輸入法

† QQ 輸入法及搜狗輸入法都是由騰訊所開發，本研究中我們分析了 QQ 輸入法，發現它含有我們先前在搜狗輸入法中發現的相同漏洞

總結來說，除了榮耀以外，我們發現的加密破解方法在經過廠商修補後，均已無效。而在榮耀手機以外廠牌的百度輸入法中，仍持續存在加密的弱點，但我們暫時還未找到方法可以利用這些弱點解密傳輸中的使用者輸入資訊。

受影響軟體列表

我們建議所有使用者保持作業系統和應用程式（包含輸入法）在最新版本，若您有使用下列軟體，我們強烈建議您檢查並安裝這些軟體及作業系統最新的更新。截至 2024 年 4 月 1 日，下列軟體已有更新可供安裝，安裝後可修補我們發現的安全漏洞。

非作業系統預載（手動安裝）的第三方開發者的輸入法：

- 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（此開發者未完整修補我們發現的漏洞，詳情見下）
- Android 平台的 iFlyTek IME / 讯飞输入法

三星中國版作業系統中預載的：

- Samsung Keyboard
- Baidu IME / 百度输入法

小米中國版作業系統中預載的：

- 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 中國版作業系統中預載的：

- Sogou IME Custom Version / 搜狗输入法定制版

Vivo 中國版作業系統中預載的：

- Sogou IME Custom Version / 搜狗输入法定制版

下列軟體仍未使用 TLS，因此可能仍有漏洞：

非作業系統預載（手動安裝）的第三方開發者的輸入法：

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

小米中國版作業系統中預載的：

- Baidu IME Xiaomi Version / 百度输入法小米版

OPPO 中國版作業系統中預載的：

- Baidu IME Custom Version / 百度输入法定制版

下列軟體含有未修補的漏洞，能夠輕易被攻擊者所利用，我們建議使用者改用其他輸入法：

非作業系統預載（手動安裝）的第三方開發者的輸入法：

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

榮耀中國版作業系統中預載的：

- Baidu IME Honor Version / 百度输入法荣耀版

綜合建議

給資安研究人員

- 資安研究人員應該多加研究東亞及其他熱門區域的手機應用程式生態系，即使這些區域並非研究人員原生的區域。
- 資安研究人員應發展更佳的動態及靜態分析方法，以利大規模尋找我們發現的此類型漏洞。
- 資安研究人員通報漏洞時應以開發者所在地區的常見語言寫出簡短摘要及郵件標題。

給應用程式商店

- 應用程式商店不應要求需註冊帳號才能下載安全性更新。
- 應用程式商店不應該根據地理位置阻擋安全性更新。
- 如同 Google Play 商店，其他應用程式商店應該提供方式讓開發者標示隱私和安全資訊，包含網路資料傳輸是否加密。
- 當開發者在應用程式商店中標示應用程式會加密所有傳輸資料時，應用程式商店應予顯示，當開發者並未如此標示時，應用程式商店亦應警告使用者。
- 應用程式商店應針對特定機敏類型的應用程式（例如輸入法）要求開發者保證所有傳輸資料均經加密，或保證不傳輸任何資料。

給輸入法開發者

- 使用經過廣泛測試的標準加密通訊協定，例如 TLS 及 QUIC。
- 儘可能將功能設計為可離線運作、不需傳輸任何敏感資料到雲端伺服器。

給手機作業系統開發者

- 如同 iOS, Android 應實作沙箱來限制輸入法程式的網路傳輸和其他危險行為，在使用者主動允許前不予放行。
- Android 及 iOS 開發者應設計更好的「網路存取」權限，讓使用者一目瞭然應用程式是否透過網路傳輸任何資料。

給手機製造商

- 將輸入法整合並預載在作業系統之前，應稽核其安全性。

給一般使用者

- 搜狗、QQ、百度、訊飛輸入法的使用者，無論輸入法是手動從應用程式商店安裝或者原本就預載在作業系統當中，應確保輸入法及作業系統維持在最新版本。
- 顧慮隱私的使用者應停用任何輸入法中的雲端功能。
- 顧慮隱私的 iOS 使用者不應啟用輸入法的「允許完整存取權」。