Hi,

Thank you for your report. We appreciate your assistance in improving our security.

We are currently taking action to address the identified flaw and would like to provide you with an update on our investigation and mitigation efforts.

1、Technical Analysis and Mitigations

1.1 Root Cause

The root cause of the security flaw was the exploitation of the leaked AES IV value which is used to encrypt the u/p/g parameters in the encrypted transmission. Attackers could use a padding oracle attack to brute-force the plaintext content of HTTP requests, which could lead to the leakage of user information under specific circumstances.

The attack mainly relied on the different HTTP response codes returned by the server-end. A 500 code indicated that AES was verified and decrypted successfully, but an error related to other business logic was encountered, while a 400 code indicated that AES verification and decryption failed.

1.2 Temporary Mitigation

To promptly mitigate the risks, we are planning to introduce temporary measures to reduce the potential impact.

Date of mitigation application: June 30th, 2023.

Description:
Currently, the server can return three types of HTTP response status codes.

- NGX_ERROR (responsed with 500)
- NGX_HTTP_BAD_REQUEST (responsed with 400)
- NGX_OK (responsed with 200

Details:
As the vulnerabilities can be exploited with different HTTP status codes, including NGX_ERROR (responsed with 500) and NGX_HTTP_BAD_REQUEST (responsed with 400), a workaround would be introduced to set all failure codes to 400. This prevents attackers from using different HTTP status codes for brute-forcing.

1.3 Security Patches and Releases

To address the security vulnerabilities, two fixing methods will be applied with the shipments of Sogou Pinyin Method security releases. Details are listed as follows:

Firstly, implementation of HTTPS. To ensure consistency with the behavior of the iOS version, all network transmissions used by Windows and Android clients will be upgraded to HTTPS.

Secondly, strengthening the initialization vector to address the security flaw in the iOS client by replacing the timestamp used to generate IV with a random number, which complies with the behavior of the Android version.

Below is the release plan for the aforementioned security fixes:

Available for	Fixed	Release date
Android	v11.25	about to release before July 20th, 2023
iOS	v11.25	about to release before July 20th, 2023
Windows	v13.7	about to release before July 30th, 2023

Please note that the fixes will be completed on July 31st, 2023. We kindly request that you refrain from disclosing any information regarding the vulnerability at this time.

2、Clarifying Data Transmission, Functionality of The Program and Privacy Policy

2.1 For Windows version, the transmission of typed text, as shown in Figure 1, is a feature of cloud-based typing app and is stated in the Privacy Agreement.

Sogou Pinyin Method is a cloud-based typing APP that offers more accurate and extensive candidate vocabularies compared to virtual keyboard apps based on local thesaurus, thus enhancing typing efficiency.

While installing, the Privacy Agreement clearly states that text information uploaded for cloud computing during using specific services is subject to user agreement. Detail of which can be found at the link below
https://rule.tencent.com/rule/preview/b692b40e-97b9-4e28-8b55-7f08d598ecec?p=privacy&f=about


搜狗输入法Windows版个人信息保护政策

发布日期：2022-01-13　生效日期：2022-01-13

引言
1.如何收集和使用您的个人信息
2. 如何使用Cookie
3. 如何共享、转让及披露您的个人信息
4. 您如何管理您的个人信息
5. 如何存储您的个人信息
6. 如何保护您的个人信息
7. 如何保护未成年人个人信息
8. 如何更新本政策
9. 如何联系我们
10. 附则
11. 关键词定义

1.如何收集和使用您的个人信息

我们会根据正当、合法、透明、最小必要的原则，基于本政策所述的目的，收集和使用您的个人信息。

为了向您提供更优质和智能的搜狗输入法Windows版产品和服务，我们可能需要收集下述信息，以下我们将详细说明本软件收集和使用的个人信息，您也可以通过《个人信息收集清单》快速查看前述信息。如果您拒绝提供，将无法享用对应的业务功能和服务。

1.1向您提供产品与服务过程中您主动提供的个人信息：

1.1.1 账户信息

①当您通过搜狗通行证登录搜狗输入法Windows版账号，您需要向我们提供您的用户名、邮箱或手机号以完成注册及登录。您也可以选择使用第三方账号登录，经过您的授权同意，第三方账号平台可能会向我们提供您的账户昵称、头像、OpenID。

②如您不登录搜狗输入法Windows版账号，我们不会收集您的上述个人信息，但与登录相关的功能将无法使用。

1.1.2 *语音信息*

①当您使用语音输入功能时，您需要向我们提供您的***语音信息***，以实现语音转写的输入功能。语音输入完成后我们不会存储您的语音信息。②当您使用录音转文字功能时，您需要向我们提供拟转写的***音频信息***，以便我们向您返回音频转写后的结果。前述音频信息及转写结果仅会在我们的服务器临时存储，您可以将音频信息及转写结果上传至个人云空间，并可随时删除云空间的内容。

1.1.3 文本内容和图像信息

①在您使用快捷翻译功能、云输入及联想功能、智能回复功能、搜索候选功能时，您需要向我们提供您输入的部分**文本信息**，以便我们为您提供更方便、快捷的输入服务。②当您使用剪贴板功能时，我们会在本地读取您的剪贴板内容，以便将您复制的内容快速粘贴上屏，提高您的输入效率。剪贴板内容不会上传到云端。③当您使用图片转文字功能时，您需要向我们提供您待转换的**图像信息**，以便我们通过图片转文字OCR功能识别图像上的**文字信息**，向您提供转化后的结果。

1.1.4 联系人信息

为了及时解决您的意见反馈、投诉或咨询本产品的相关问题，您需要向我们提供真实的联系方式，以及问题相关的证明材料（包括图片、视频或文本信息）。此外，请您知悉，系统可能会记录您与客服之间的沟通记录、处理方案及结果。如您不提供上述信息，我们可能无法核验身份、定位问题并向您及时反馈。

1.2 向您提供产品与/或服务过程中我们主动收集的个人信息

1.2.1 设备信息

为了使搜狗输入法Windows版应用与设备进行必要的适配并安全服务，在您使用本应用时，根据您授予的具体权限，我们会收集您的设备型号、CPU硬件类型、硬件UUID、CPU架构、系统版本、屏幕分辨率。收集这些信息是为了帮助我们进行bug分析，保障您正常使用本应用的服务、改进和优化我们的产品体验、保障您的账号安全。我们不会将该等信息与您的个人身份信息进行匹配，除本政策另有明确约定外，我们也不会将您的设备信息提供给任何第三方。

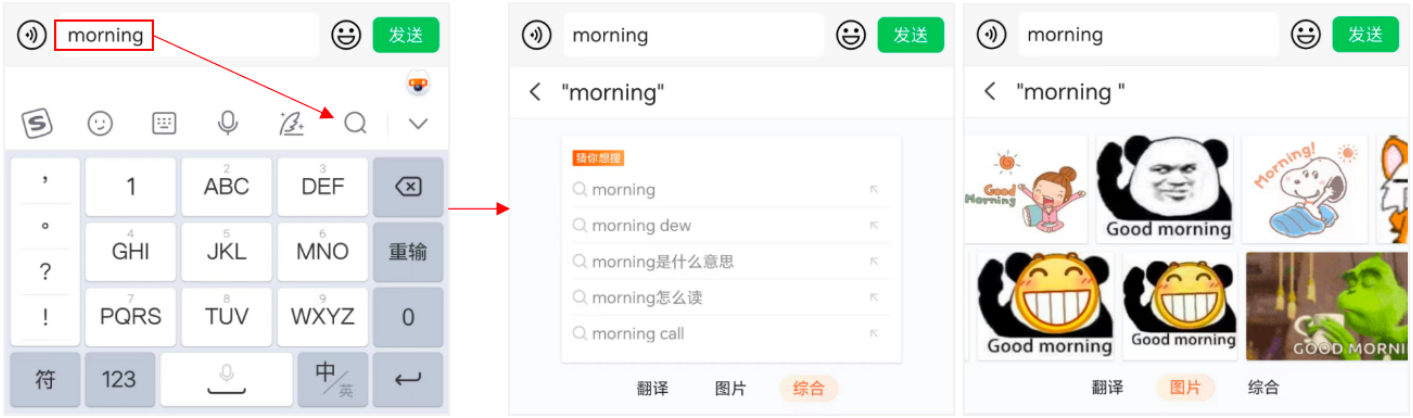
1.2.2 *日志信息*

当您使用搜狗输入法Windows版产品与服务时，我们会收集您的相关软件崩溃、系统活动信息、软件设置记录、IP地址信息，以便于我们改善产品与服务，给您更好的服务体验。请您注意，基于确保搜狗输入法客户端使用安全的目的，我们会读取您的输入法列表、电脑软件进程信息，以分析排查软件崩溃问题、防止被其他恶意仿冒程序实施界面劫持攻击，同时以便为您提供对应的下载、安装或升级服务。

As Chinese is a pictographic language, users need to input pinyin strings before receiving candidate Chinese characters. For example, to type "你好 (Hello)" in Chinese, users need to input the pinyin characters "Nihao" first. Additionally, due to the polyphonic nature of Chinese characters, users need to input pinyin strings and rely on the computing power of the cloud to return correct candidate characters for fast and accurate typing. For instance, the Chinese character "行" can have different pronunciations, such as "xíng" in the vocabulary "行走" and "háng" in "行列".

2.2. In the Android version of Sogou Pinyin Method, the transmission of typed text, as shown in Figure 3, is necessary when using the built-in search engine services indicated by the magnifying glass icon.

Sogou Pinyin Method offers built-in search engine services in its Android version, accessible by clicking the magnifying glass icon as shown in Figure below.



By using this feature, users can directly query translations, expressions, and interpretations online without switching to search engine web pages or other apps.

During this process, the text in the input box is included in the sent HTTP requests and the server returns the results after retrieval. It is necessary for the search function to work.

This behavior is stated in clause 1.1.3 of the Privacy Agreement


搜狗输入法Windows版个人信息保护政策

发布日期：2022-01-13　生效日期：2022-01-13

引言

1.如何收集和使用您的个人信息

2. 如何使用Cookie

3. 如何共享、转让及披露您的个人信息

4. 您如何管理您的个人信息

5. 如何存储您的个人信息

6. 如何保护您的个人信息

7. 如何保护未成年人个人信息

8. 如何更新本政策

9. 如何联系我们

10. 附则

11. 关键词定义

1.如何收集和使用您的个人信息

我们会根据正当、合法、透明、最小必要的原则，基于本政策所述的目的，收集和使用您的个人信息。

为了向您提供更优质和智能的搜狗输入法Windows版产品和服务，我们可能需要收集下述信息，以下我们将详细说明本软件收集和使用的个人信息，您也可以通过《个人信息收集清单》快速查看前述信息。如果您拒绝提供，将无法享用对应的业务功能和服务。

1.1向您提供产品与服务过程中您主动提供的个人信息：

1.1.1 账户信息

①当您通过搜狗通行证登录搜狗输入法Windows版账号，您需要向我们提供您的用户名、邮箱或手机号以完成注册及登录。您也可以选择使用第三方账号登录，经过您的授权同意，第三方账号平台可能会向我们提供您的账户昵称、头像、OpenID。

②如您不登录搜狗输入法Windows版账号，我们不会收集您的上述个人信息，但与登录相关的功能将无法使用。

1.1.2 *语音信息*

①当您使用语音输入功能时，您需要向我们提供您的***语音信息***，以实现语音转写的输入功能。语音输入完成后我们不会存储您的语音信息。②当您使用录音转文字功能时，您需要向我们提供拟转写的***音频信息***，以便我们向您返回音频转写后的结果。前述音频信息及转写结果仅会在我们的服务器临时存储，您可以将音频信息及转写结果上传至个人云空间，并可随时删除云空间的内容。

1.1.3 文本内容和图像信息

①在您使用快捷翻译功能、云输入及联想功能、智能回复功能、搜索候选功能时，您需要向我们提供您输入的部分**文本信息**，以便我们为您提供更方便、快捷的输入服务。②当您使用剪贴板功能时，我们会在本地读取您的剪贴板内容，以便将您复制的内容快速粘贴上屏，提高您的输入效率。剪贴板内容不会上传到云端。③当您使用图片转文字功能时，您需要向我们提供您待转换的**图像信息**，以便我们通过图片转文字OCR功能识别图像上的**文字信息**，向您提供转化后的结果。

1.1.4 联系人信息

为了及时解决您的意见反馈、投诉或咨询本产品的相关问题，您需要向我们提供真实的联系方式，以及问题相关的证明材料（包括图片、视频或文本信息）。此外，请您知悉，系统可能会记录您与客服之间的沟通记录、处理方案及结果。如您不提供上述信息，我们可能无法核验身份、定位问题并向您及时反馈。

1.2 向您提供产品与/或服务过程中我们主动收集的个人信息

1.2.1 设备信息

为了使搜狗输入法Windows版应用与设备进行必要的适配并安全服务，在您使用本应用时，根据您授予的具体权限，我们会收集您的设备型号、CPU硬件类型、硬件UUID、CPU架构、系统版本、屏幕分辨率。收集这些信息是为了帮助我们进行bug分析，保障您正常使用本应用的服务、改进和优化我们的产品体验、保障您的账号安全。我们不会将该等信息与您的个人身份信息进行匹配，除本政策另有明确约定外，我们也不会将您的设备信息提供给任何第三方。

1.2.2 *日志信息*

当您使用搜狗输入法Windows版产品与服务时，我们会收集您的相关软件崩溃、系统活动信息、软件设置记录、IP地址信息，以便于我们改善产品与服务，给您更好的服务体验。请您注意，基于确保搜狗输入法客户端使用安全的目的，我们会读取您的输入法列表、电脑软件进程信息，以分析排查软件崩溃问题、防止被其他恶意仿冒程序实施界面劫持攻击，同时以便为您提供对应的下载、安装或升级服务。

2.3.The Cloud Thesaurus function requires information on installed apps, as outlined in clause 1.2.8 of the Privacy Agreement.

To provide more accurate candidate words, the Sogou Pinyin Method offers users candidate words from different industry categories and scenarios based on the apps installed on their device. This feature is called the Cloud Thesaurus and has been proven to improve the typing experience.

For instance, if a user has installed a certain game on their Android device, the Sogou Pinyin Method will suggest terms related to the characters in that game.
Detail of which can be found at the link below：

https://shouji.sogou.com/wap/htmls/privacy_policy.html

If you have more concerns or suggestions, please let us know.

Best wishes,
Sogou Pinyin Method Team