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 (responded with 500)
- NGX_HTTP_BAD_REQUEST (responded with 400)
- NGX_OK (responded with 200)

Details:
As the vulnerabilities can be exploited with different HTTP status codes, including NGX_ERROR (responded with 500) and NGX_HTTP_BAD_REQUEST (responded 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:

<table>
<thead>
<tr>
<th>Available for</th>
<th>Fixed</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>v11.25</td>
<td>about to release before July 20th, 2023</td>
</tr>
<tr>
<td>iOS</td>
<td>v11.25</td>
<td>about to release before July 20th, 2023</td>
</tr>
<tr>
<td>Windows</td>
<td>v13.7</td>
<td>about to release before July 30th, 2023</td>
</tr>
</tbody>
</table>

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-97b9-4e28-8b55-7f08d598ecce?p=privacy&f=about
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.

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