Security issue in LINE’s group note API resolved

2019.08.01

2019年8月15日更新: 於下方新增中文版說明

2019-08-15 Update: Added Chinese translation version at the bottom.

On July 25t, 2019 we received a report about a security bug (vulnerability) affecting LINE's group note API sever, and promptly resolved the issue.

This announcement details our response.

1. Overview of the vulnerability

There was an improper access control issue in LINE's group note API server, in particular in the social graph retrieval API. This issue allowed third parties to obtain the internal identifiers of other LINE users (*1) one has interacted with on the LINE platform. Following are the details of the vulnerability and the social interactions that could lead to users being affected.

Vulnerability Details

Under certain conditions, the following information, related to social relationships between LINE users (*2), were obtainable from the social graph retrieval APIs:

- Group identifiers
  - Our system automatically creates an internal group identifier, when an album or a note shared with another LINE user is created. This group identifier could be obtained by abusing this vulnerability.
  - This group identifier is also generated beforehand as part of the note or album creation process, for certain versions of the LINE application.
  - Therefore, users who viewed notes or albums within a chat room may be affected. In some cases, simply opening a chat room with linked notes or albums may expose users to this vulnerability.
- User identifiers of socially related peer users
  - When a group identifier is created, the user identifiers of all members of the group are associated with the created group identifier. As a result of this vulnerability, it was possible to obtain the user identifiers of all group members, if the group identifier was known.
  - The user identifiers obtainable as a result of this vulnerability are generally those of the target user's LINE friends. However, depending on the conditions under which the group identifier was created, the list of retrieved identifiers might contain identifiers belonging to other LINE users that the target user is in a social relationship with (*2).

    - In light of this, the vulnerability allowed someone abusing this vulnerability to get information about the relationships of users on their friends list ("Friends of friends"). In some cases, this type of data could also be acquired for unrelated users, as described above.

(*1) In some cases a third party might be able to obtain internal identifiers without being registered as a friend of the target user.

(*2) The relationships explained above will be referred to as *social relationship(s)* for the rest of this article. Social relationships include unidirectional and bidirectional LINE friendship relations, being invited in the same chat room or group, sharing notes or albums with other LINE users.

2. Our response

We discovered the cause of the vulnerability and deployed a fix on July 29th, at 11:21 AM JST.

After investigating our internal access logs, as well as the details of the vulnerability, we have found that up to 695,192 users may have been affected.

The reasons behind the number being higher than expected for this kind of vulnerability are:

- The reporter created a public LINE Bot for the purpose of demonstrating the effect of this vulnerability.
- This bot was added as a friend by multiple users, which allowed them to view information about other users' social relationships (*2), including users not currently on their friends list.

By creating the bot, and making it available to other users, the reporter was violating of the Terms and Conditions of LINE’s Bug Bounty Program. We have received a written pledge from the researcher stating that any additional data acquired has not been made publicly available, and has been deleted.

Neither the contents of notes nor conversations was leaked due to this issue.

In addition, the bot is currently suspended, as part of our incident response handling.

Affected Users

The following two types of users are affected:

Note: LINE Bot in the following explanations refer exclusively to the Bot created by the reporter of this vulnerability.

> LINE Users (A) who had their contact details shared in the LINE Bot's chat-room (by using the 'Share Contact' function) by Line User (X) , who previously added the LINE Bot.
>
> LINE Users (B) who were in a social relationship with LINE Users (A), and who meet the specific requirements mentioned in the Vulnerability Details section above.

Number of affected users by Country / Region:

Japan: 328,468

Taiwan: 327,728

Other: 13,652

Other (*): 25,334

Total: 695,192

(*) Inactive accounts etc.

3. Vulnerability timeline

- July 25th, 2019 03:03: Vulnerability report received through LINE Security Bug Bounty Program
- July 29th, 2019 11:21: Vulnerability fixed.
- July 30th, 2019 18:53: Informed reporter that the reported vulnerability has been fixed.
- July 30th, 2019 21:58: Received a written oath confirming that the reporter has deleted all data acquired as a result of exploiting this vulnerability

All times are in JST (UTC+9).

4. About LINE's Bug Bounty Program

We continue to accept vulnerability reports via the LINE Security Bug Bounty Program.

As of June 2019 the following vulnerabilities have been recognized as valid:

https://linecorp.com/en/security/article/213
https://bugbounty.linecorp.com/en/halloffame/

To keep the operations of LINE Group transparent, we will continue to disclose significant vulnerabilities.

We appreciate the researcher sharing information regarding this vulnerability with us, but because the researcher acted in violation of the **Terms of Use** of LINE’s Bug Bounty Program, we were unable to award a bounty.

5. Inquiry

Inquiry form : **https://contact-cc.line.me/en/10095/** (until August 31st 2019)

「LINE」API伺服器在特定條件下可能取得用戶清單之弱點修正通知

2019年7月25日，透過「LINE資安漏洞回報獎金計畫」，接獲LINE群組記事本功能之API伺服器安全弱點（脆弱性）報告，因此特此通知已修正該安全弱點。

1.弱點概要

先前，LINE群組記事本功能所使用可取得LINE用戶間社交關係的API中，存在存取控制弱點。
透過此弱點，第三者可取得與LINE用戶在特定條件下交流之其他使用者（※1）的內部識別碼。(該弱點已經修正，請參考「2.相關因應 」)

※1 也會發生在已加入好友以外之情況

因弱點而可能取得之資訊

針對任一LINE用戶在特定條件下可取得之社交關係（※2 ），如下所示：

- 群組識別碼
    - LINE用戶與其他用戶建立記事本或相簿時，內部會自動產生群組識別碼。本群組識別碼可透過此弱點取得。
    - 此識別碼依使用的LINE APP版本，即使在準備建立記事本或相簿的階段也會建立。
    - 因此，在「移至聊天室內的記事本或相簿功能」、「已開啟聊天室」等條件下，也可能已經建立群組識別碼。
- 具有社交關聯性的用戶識別碼
    - 已建立群組識別碼時，可透過弱點取得該群組內的其他用戶識別碼。
    - 此識別碼在大多數情況下是具有好友關係中的使用者識別碼，但是依建立群組識別碼時的條件，也包含非好友的情況。

※2 以上所述之關係本文將稱之為「社交關係」。社交關係指的是在LINE中被邀請進入同一聊天室或群組，因此能共用記事本和相簿的用戶，這包括「單向」和「雙向」的好友關係。

2.相關因應

2019年7月29日11:21，已查明弱點原因並完成修正。

經調查該弱點及存取紀錄，已知結果：

- 回報者為了證實此弱點，自己製作了LINE Bot。
- 該回報者透過數個用戶將上述LINE Bot加入好友，使得包含非好友關係的社交關係變成可顯示於LINE Bot。
- 因可顯示在LINE Bot上而受到影響的用戶，最多達695,192用戶。

由於該弱點回報者違反「LINE資安漏洞回報獎金計畫」之規定，因此已給予嚴重警告，並收到其同意刪除且禁止洩漏所取得資訊之相關承諾書。

另外，並無因本事件而洩漏聊天內容或記事本內容等之事實。並且該LINE Bot已遭停權無法使用。

受影響用戶

下列情形之**LINE用戶(A)、LINE用戶(B)**，可能成為受影響用戶

- LINE用戶(X)將利用上述弱點之特定LINE Bot加入好友，於該LINE Bot的聊天室，使用聯絡資訊分享功能而被分享的**LINE用戶(A)。**
- 以**LINE用戶(A)**而言，在前述**「因弱點而可能取得之資訊」**之特定條件下，與其有社交關係的**LINE用戶(B)。**

依國家/ 地區分類，受影響用戶數的詳細內容

日本：328,468　台灣: 327,728　其他國家/地區：13,652　其他(*)：25,344
合計：695,192

(*)非活躍帳號等

3.自發現弱點起，因應的時間順序如下（日本時間）

- 2019年7月25日03:03，透過「LINE資安漏洞回報獎金計畫」接受到弱點回報
- 2019年7月29日11:21，弱點修正完畢
- 2019年7月30日18:53，告知回報者已處理完畢
- 2019年7月30日21:58，取得回報者之資訊刪除相關承諾書

4.關於LINE資安漏洞回報獎金計畫

「LINE資安漏洞回報獎金計畫」日後仍將持續接受弱點回報。2019年6月當時之弱點認定，如以下公告所示：

https://linecorp.com/ja/security/article/212
https://bugbounty.linecorp.com/ja/halloffame/

LINE集團為了保持透明性，日後亦將持續發佈影響重大的弱點回報與修正報告。

另外，關於本案件，因違反「LINE資安漏洞回報獎金計畫」之規定，故不支付回報獎金。

5.本案件洽詢

本案件相關問題請洽詢：**https://contact-cc.line.me/detailId/10095**(2019年8月31日止)

以上