「LINE」のAPIサーバーにおける特定条件下でユーザーリストが取得可能な脆弱性の修正のお知らせ

2019.08.01

2019年7月25日にLINE Security Bug Bounty Programを通じて LINEのグループノート機能のAPIサーバーにおけるセキュリティバグ（脆弱性）報告を受け、その修正を行なったことをお知らせいたします。

1. 脆弱性の概要

LINEのグループノート機能では、LINEユーザー間のソーシャル関係を取得するAPIを用いています。このAPIにおいて、アクセス制御の不備がありました。
これにより、LINEユーザーと特定の条件で交流関係が生じていた他の利用者(※1)の内部識別子が、第三者から取得可能な状態となっていました。

※1 友だち登録されている場合以外にも該当するケースがあります

脆弱性によって取得可能だった情報

任意のLINEユーザーに対して、特定の条件下で取得可能だったソーシャル関係の定義は以下の通りです。

- グループの識別子
  - LINEユーザーが他のユーザーとの間に、ノートまたはアルバムを作成した際に、内部的にグループの識別子が自動で作成されます。このグループの識別子が脆弱性によって取得可能となっていました。
  - この識別子は、利用しているLINEアプリのバージョンによっては、ノート又はアルバムを作成する準備段階でも作成されます。
  - そのため「トークルーム内のノートまたはアルバム機能に遷移した」「トークルームを開いた」といった条件でも、グループの識別子が作成されていることがあります。
- 交流関係にある他のユーザーの識別子
  - グループの識別子が作成されている場合、そのグループの対象となる、他のユーザーの識別子が脆弱性によって取得可能となっていました。
  - この識別子は、多くの場合、友だち関係にある利用者の識別子となります。ただし、グループの識別子の作成時の条件によっては、友だちではないケースも含まれます。

2. 対応について

2019年7月29日 11:21に、脆弱性の原因を特定し、修正を完了しています。

当該脆弱性およびアクセスログの調査を行った結果、

- 当該脆弱性を報告したセキュリティ研究者自身がこの脆弱性を実証する目的でLINE Botを作成していた
- 作成されたLINE Botを友だち追加した複数のユーザーによって、友だち関係ではないLINEユーザーも含むソーシャル関係がLINE Bot上に表示可能な状態となった

- LINE Bot上に表示可能な状態になったとして影響を受けたユーザーは、最大で695,192ユーザーであった

ということがわかりました。

当該セキュリティ研究者に対しては、Bug Bounty Programの規約違反行為に該当するとして厳重注意を行い、取得した情報の廃棄と漏洩の禁止に関する誓約書を受領しています。

なお、この件に起因して、トーク内容やノートの内容などが漏洩した事実はございません。また、当該LINE Botはすでに利用不可能な状態となっております。

影響を受けたユーザー

以下に当てはまる **LINEユーザー(A)、LINEユーザー(B)** が影響を受けたユーザーとなります

- 本脆弱性を利用した特定のLINE Botを友だち追加していたLINEユーザー(X)が、当該LINE Botのトークルームで、連絡先共有機能を使って共有された **LINEユーザー(A)**
- 上記LINEユーザー(A)からみて、上述の **「脆弱性によって取得可能だった情報」** に示す特定の条件下で交流関係が生じていた他の利用者 **LINEユーザー(B)**

影響を受けたユーザー数の国家 / 地域別の内訳

日本: 328,468　台湾: 327,728　他の国家/地域: 13,652　その他(*): 25,344
合計: 695,192

(*)休眠アカウントなど

3. 脆弱性発覚からの対応時系列（日本時間）

- 2019年7月25日 03:03 LINE Security Bug Bounty Programを通じた脆弱性の報告
- 2019年7月29日 11:21 脆弱性の修正を完了
- 2019年7月30日 18:53 報告者に対して対応完了を連絡
- 2019年7月30日 21:58 報告者から情報削除についての誓約書を受領

4. LINE Security Bug Bounty Programについて

LINE Security Bug Bounty Programでは、引き続き脆弱性の報告を受け付けております。2019年6月現時点における脆弱性の認定は以下の通りです。

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

LINEグループでは透明性を保つため、重要な脆弱性は今後も公開を検討してまいります。

なお本件に関しましては、Bug Bounty Program の規約違反を理由に、報奨金の支払いは行っていません。

5. 本件に関するお問い合わせ

お問い合わせフォーム： **https://contact-cc.line.me/detailId/10095** (2019年8月31日まで)

以上