Notice regarding unauthorized friend requests and group chat invitations on the LINE app

2020.11.17

(Chinese and Bahasa follow English)

All times are in JST unless noted otherwise

1. Overview

We have detected bots(*1) appearing as dedicated CLOVA accounts(*2) that have sent a large number of unauthorized friend requests and group chat invitations to LINE users from October 15, 2020 at 17:00 to November 3, 2020 at 10:00. We apologize for any inconvenience experienced by our users.

The details of our investigation and response to the issue are summarized below.

(*1) Bots are functions that provide automatic responses and translation

(*2) A dedicated CLOVA account is a LINE account to be used with LINE's CLOVA Assistant which has a feature that allows users to send LINE messages by dictating them and having new LINE messages spoken out loud. Adding a dedicated CLOVA account as a LINE friend is necessary to enable this feature.

2. Incident assessment

According to our investigation, the abuse of a software bug caused the bots to send the friend requests to users. We can confirm that no accounts were compromised and no information was leaked due to the incident.

・Duration: Between October 15, 2020 at 17:00 to November 3, 2020 at 10:00

・Number of bots that send friend requests and group chat invitations: 7,768

・Breakdown of affected users:

Japan: 15,530

Taiwan: 87,197

Thailand: 2,813

Indonesia: 7,084

Other: 8,597

Total: 121,221

We remind our users that LINE Official Accounts(*3) and other accounts managed by LINE are never used to send messages or friend requests to users without their consent.

(*3) LINE Official Accounts are LINE accounts used by companies to send notifications to their subscribed users.

3. Cause of incident and our response

The causes and response status of this incident are as follows.

Discovery of incident

On October 15, 2020, LINE received a report of the bug that caused this incident through the LINE Security Bug Bounty Program.

According to our assessment, through certain APIs associated with "CLOVA Assistant," unauthorized friend requests were sent from bots appearing as dedicated CLOVA accounts. (At the time of this announcement, we have fixed the issue by applying a patch on the APIs.)

According to the individual who discovered the vulnerability, the LINE account belonging to the individual had added a number of accounts not recognized by the individual.

While we continue to investigate this issue, we believe that this vulnerability was discovered by others which led to others taking advantage of this vulnerability from November 2, 2020.

LINE would like to make clear that, at the moment, we are not aware of any evidence associating the individual who discovered this vulnerability with those who took advantage of it.

Regarding affected users

We estimate that the users affected by this incident were targeted using a list of internal identifiers of LINE, which were previously obtained by the person who committed the abuse. This was done by using user information that was collected by, for example, joining a common LINE group, searching for a user by phone number or LINE ID, or collecting public information on user activities on other LINE services.

Since the user information that could be obtained through the bot was limited to affected users' public information (display name, profile image, status message, etc.), no additional information leakage had occurred due to this incident.

Our response

The bots that caused this incident is currently being deleted.

For customers who have been invited to many groups, we have cancelled open requests to join groups(*4).

If you have already joined a group, it will not be deleted automatically. Therefore we sincerely apologize for the inconvenience, but we ask that affected users leave the group/s.

(*4) If you have already joined a group, you will need to leave the group manually.

4. Correspondence in chronological order

October 15, 2020, 17:56: Received a report about the bug via the LINE Bug Bounty Program

October 29, 2020, 18:15: Received a user report about a dedicated CLOVA account adding the user as a friend and inviting the user into a group chat

November 2, 2020, 10:38: Confirmed that a CLOVA Assistant API had been used to make a large number of calls

November 2, 2020, 16:00: 14 bots appearing as dedicated CLOVA accounts were removed

November 2, 2020, 20:30: First CLOVA Assistant API patch distributed

November 3, 2020, 13:39: A notification about a service interruption to the CLOVA Assistant service announced on Twitter (interruptions occurred on November 2, from 11:40 to 13:51 and from 19:18 to 22:17)

November 4, 2020, 19:00: Cancelled first batch of group chat invitations sent by the bots

November 4, 2020, 20:05: Second CLOVA Assistant API patch distributed

November 5, 2020, 19:00: Cancelled second batch of group chat invitations sent by the bots

November 16, 2020, 15:46: Cancelled third batch of group chat invitations sent by the bots

November 17, 2020, 19:40: Notification sent to users who received a large number of unauthorized friend requests in Japan, Indonesia and other regions via LINE's Official Account

November 18, 2020, 11:35: Notification sent to users in Taiwan via LINE's Official Account

November 18, 2020, 17:30: Cancelled fourth batch of group chat invitation sent by bots

November 18, 2020, 20:10: Notification sent to users in Thailand via LINE's Official Account

November 20, 2020, 10:30: Cancelled fifth batch of group chat invitation sent by bots

November 24, 2020, 17:42: Second notification sent to all affected users in Japan, Taiwan, Indonesia, Thailand and other regions

5. Regarding bug reports

Notice to security researchers

LINE has been accepting bug reports via the LINE Security Bug Bounty Program since 2016 and offers bounties according to its guidelines.

While this incident is attributed to the vulnerability discovered in our service, our priority is to ensure the safety of our users and continued operation of services. We ask for your understanding and cooperation with regards to the following:

- We strive to fix all vulnerabilities as quickly as possible, and depending on the issue it may take some time to develop a fix.
- When verifying vulnerabilities, please use your own account or obtain the consent of a trusted collaborator in order to avoid endangering other user accounts.
- Please avoid sharing to third parties in order to prevent the risk of further exploitation until the vulnerability can be fixed.
- Vulnerabilities resulting in spam or denial-of-service may take longer to fix due to consideration of potential repercussions from countermeasures.

Once a vulnerability is discovered, please promptly report the bug to LINE. The **Prohibited Acts** section in our **Terms of Use** strictly prohibits the sharing, leaking or otherwise disclosing any such information to third parties or verify using other accounts. In the event of a violation to the terms, we have the right to refuse bounty payment and exclude the participant from future participation in the LINE Security Bug Bounty Program. If a violation is discovered, the disclaimer for verifying the vulnerability will no longer apply, and criminal charges may be made for unauthorized access or denial of service.

Notice to users who have discovered vulnerabilities on LINE

Please refrain any act that may harm other users, even if such methods are publicly available. We will take strict measures to ensure that neither our users nor our service are negatively impacted.

If you discover a security vulnerability on LINE, please report it to the LINE Security Bug Bounty Program. In the event a vulnerability is discovered by another individual, you may still be eligible for a reward if the information is new and deemed valuable by LINE. Please specify in your report if a vulnerability is discovered by another individual.

6. Update history

November, 17, 2020: Notification posted in Japanese, English, Chinese and Bahasa

7. Inquiries regarding this matter

For users with individual LINE accounts who have inquiries related to this matter, please contact us using the following form by selecting "Other" for Question #2: **https://contact-cc.line.me/detailId/10666**

陌生官方帳號主動加為好友或陌生群組邀請之事件說明

1. 事件概要

2020年10月15日台灣時間16:00至11月3日09:00間，曾發生用戶在沒有同意的情況下，CLOVA相關的灰盾陌生官方帳號主動加入用戶為好友或邀請加入群組，若因此事件造成您的困擾，我們感到十分抱歉。

本文說明我們對此事件的調查與應對。

2. 事件評估

經我們的調查發現，有濫用者發現軟體漏洞並利用此漏洞將用戶加入陌生官方帳號。此事件中並無任何LINE帳號被竊取或密碼遭到洩漏等情況。

・影響期間： 2020年10月15日台灣時間16:00至11月3日09:00

・有自動加入好友或邀請加入群組功能的帳號數量：7,768

・受此事件影響的各國用戶數：

日本　15,530

台灣　87,197

泰國　2,813

印尼　7,084

其他　8,597

總計：121,221

我們也想在此特別提醒用戶，在未取得用戶的同意前，LINE官方帳號決不會自動將用戶加入為好友或單方面的傳送訊息。

3. 事件的發生原因以及應對措施

有關本次事件的發生原因和應對措施簡述如下。

關於本次事件的發生經過

2020年10月15日我們透過「資安漏洞回報獎勵計劃」收到造成本次事件發生的漏洞回報。

我們的評估驗證後，發現有透過特定CLOVA助理API開發出來的Bot，這些Bot以「CLOVA專用」的官方帳號形式出現，主動將用戶加為好友。（現在我們已修復這些API）

根據回報者所述，回報者本人的LINE帳號中出現一些陌生官方帳號。

當我們持續追查後，發現此漏洞是由他人所找出。同時，我們也留意到自2020年11月2日起開始有人惡意利用此漏洞。

我們想特別強調，事件調查至此時，我們並未查出此漏洞的回報者與那些惡意利用者之間有任何關係。

本次事件中受影響的用戶

本次事件對受影響的用戶造成不便，因為此漏洞透過電話號碼或LINE ID直接搜尋用戶並在用戶尚未同意之下加為好友。

由這些Bot取得的用戶資訊僅限於用戶選擇公開之內容，例如帳號上公開顯示之姓名、個人圖片、狀態消息等，沒有其他資訊因此外洩。

我們的應對措施

引發本次事件的Bot目前已刪除完畢。

針對被邀請加入陌生群組的用戶，我們已刪除群組邀請。

若用戶已加入陌生群組，我們便無法協助刪除，懇請用戶手動操作，退出這些群組。

4. 本事件發生的時間序列（以下為台灣時間）

2020年10月15日16:56　我們透過「資安漏洞回報獎金計畫」收到一份漏洞回報。

2020年10月29日17:15　收到來自用戶的檢舉，顯示有一CLOVA相關的灰盾陌生官方帳號主動加入用戶為好友並邀請加入群組

2020年11月2日 9:38　發現單一特定CLOVA助理API有大量不當使用情形

2020年11月2日 15:00　刪除14個顯示為CLOVA專用帳號的Bot

2020年11月2日 19:30　第一次修復CLOVA助理API

2020年11月3日 12:39　在Twitter上發布CLOVA助理發生服務中斷的通知（服務中斷發生期間：11月2日 10:40至12:51、18:18至21:17）

2020年11月4日 18:00　刪除第一批由這些Bot發出的群組邀請

2020年11月4日 19:05　第二次修復CLOVA助理API

2020年11月5日 18:00　刪除第二批由這些Bot發出的群組邀請

2020年11月16日 14:46　刪除第三批由這些Bot發出的群組邀請

2020年11月18日 10:35　透過LINE系統官方帳號通知受影響的用戶

2020年11月18日 16:30　刪除第四批由這些Bot發出的群組邀請

2020年11月20日 09:30　刪除第五批由這些Bot發出的群組邀

2020年11月24日 16:42　透過LINE系統官方帳號通知第二批受影響的用戶

5. 關於LINE「資安漏洞回報獎金計畫」

請參與此計畫的資安研究人員留意

LINE 於2016年宣布長期舉辦「資安漏洞回報獎金計畫」並根據計畫規範，為回報者提供舉報獎勵。

此次事件的事發原因首先在於LINE服務上出現安全漏洞，但為保護LINE全體用戶並讓用戶順利使用服務，敬請回報者留意並理解以下注意事項：

- 我們在收到安全漏洞回報之後會立即著手修復，修復時間的長短依不同安全漏洞而定。
- 在您驗證安全漏洞時，請使用自己的帳號，若要請可信任的朋友協作時，請務必先取得對方的同意，請避免影響到他人的帳號。
- 在安全漏洞修復前，敬請留意，勿向第三者洩漏您所回報的安全漏洞，勿對外擴散。
- 會造成大量濫用或會導致帳號遭封鎖的安全漏洞，修復時間可能較長，因為我們必須避免防範機制可能產生的不良影響。

當您發現安全漏洞時，請立即透過「資安漏洞回報獎金計畫」向LINE回報。「資安漏洞回報獎金計畫」的規範明列禁止事項，包括向他人洩漏安全漏洞、以任何手法傳散給第三方、或利用他人的帳號驗證弱點。回報者如違反規範，我們有權利拒絕支付舉報奨金，也有權利將違反者排除在此計劃之外。回報者如違反規範，免責條例將不適用，且可能須負不當存取或妨礙服務等刑事之責。

請一般用戶留意

請避免對其他用戶的帳號造成影響，即使這些方式已在網路上公開。當我們發現有安全漏洞會對用戶或服務造成負面影響時，我們必會採取嚴謹的對應措施。

若您在LINE上面發現安全漏洞，請立即透過「資安漏洞回報獎金計畫」向LINE回報。即使已有其他人回報此安全漏洞，若您可以提供更新的資訊情報、或是對LINE非常有價值的分析，還是有可能獲得舉報獎勵。敬請您在回報時載明此安全漏洞是否由其他人發現。

6. 更新紀錄

2020年11月17日公開

7. 若您對於此事件仍有擔憂，請聯繫客服

若您對於此事件仍有擔憂，歡迎您聯繫我們的客服團隊。請使用個人LINE帳號進入： **https://contact-cc.line.me/detailId/10666**，請在問題2中選擇「其他」。

Pemberitahuan terkait permintaan pertemanan dan undangan grup tak resmi di aplikasi LINE

(Semua keterangan waktu terlampir berada dalam zona waktu Jepang kecuali ada informasi lain)

1. Ikhtisar

Pada 15 Oktober 2020 pukul 17:00 hingga 3 November pukul 10:00, kami mendeteksi adanya bots(*1) mencurigakan yang mengatasnamakan akun-akun ClOVA(*2) yang telah mengirimkan banyak permintaan pertemanan dan undangan tak resmi untuk bergabung ke dalam grup kepada para pengguna LINE. Kami memohon maaf atas ketidaknyamanan yang telah terjadi.

(*1) bots merupakan fungsi yang pada awalnya menyediakan respon otomatis ke pesan dari pengguna, seperti layanan penerjemahan bahasa.

(*2) Akun khusus yang didedikasikaan untuk CLOVA merupakan akun LINE yang digunakan dengan Asisten CLOVA LINE yang memungkinkan pengguna mengirimkan dan membaca pesan melalui perintah suara. Untuk mengaktifkan fitur ini, akun CLOVA harus ditambahkan.

2. Asesmen Insiden

Berdasarkan penyelidikan kami, penyalahgunaan software bug telah mengakibatkan pengiriman permohonan pertemanan oleh bot kepada pengguna. Kami mengkonfirmasi bahwa tidak ada akun yang teretas dan tidak ada informasi yang bocor pada saat kejadian berlangsung.

- Periode kejadian: tanggal 15 Oktober 2020 pukul 17:00 sampai dengan 3 November 20220 pukul 10:00
- Jumlah bots yang ditambahkan atau diundang sebagai teman: 7,768
- Jumlah pengguna terdampak berdasarkan negara/wilayah: (Total 121.221)

    Jepang: 15,530

    Taiwan: 87,197

    Thailand: 2,813

    Indonesia: 7,084

    Lainnya: 8,597

Perlu kami informasikan bahwa LINE Official Account(*3) dan akun lainnya yang dikelola oleh LINE tidak pernah digunakan untuk mengirimkan pesan atau permintaan pertemanan kepada pengguna tanpa seizin pengguna.

(*3) LINE Official Account merupakaan akun LINE yang digunakan oleh para perusahaan untuk mengirimkan pemberitahuan mengenai produk mereka kepada penggunanya masing-masing.

3. Penyebab permasalahan dan tindakan kami

Penyebab permasalahan dan tindakan kami atas permasalahan yang ada adalah sebagai berikut:

Penemuan permasalahan

Pada tanggal 15 Oktober 2020, LINE telah menerima laporan tentang adanya bug yang menyebabkan permasalahan ini melalui LINE Security Bug Bounty Program.

Berdasarkan penyelidikan kami, melalui beberapa API yang terasosiasi dengan “CLOVA Assistant,” beberapa permohonan pertemanan yang tidak sah dikirimkan dari bot yang muncul sebagai akun

khusus CLOVA. (Pada saat pengumuman ini, kami telah memperbaiki masalah tersebut dengan menerapkan tambalan pada API dimaksud).

Menurut individu yang menemukan kerentanan dimaksud, akun LINE milik individu tersebut telah menambahkan sejumlah akun yang tidak dikenali oleh individu tersebut.

Pada saat penyelidikan dilakukan, kami percaya bahwa kerentanan tersebut juga telah ditemukan oleh individu-individu lain yang mengakibatkan pihak-pihak tertentu mengambil keuntungan dari kerentanan dimaksud sejak tanggal 2 November 2020.

LINE perlu menginformasikan bahwa, pada saat ini, kami tidak mempunyai suatu bukti yang mengaitkan individu yang menemukan kerentanan tersebut dengan mereka yang mengambil keuntungan dari padanya.

Mengenai para pengguna yang terdampak

Kami memperkirakan bahwa para pengguna yang terdampak dari permasalahan ini adalah mereka yang terdapat pada daftar pengidentifikasi internal LINE yang sebelumnya didapat oleh individu yang menyalahgunakannya. Hal ini dilakukan dengan menggunakan informasi pengguna yang didapatkan melalui beberapa cara, seperti bergabung ke dalam grup LiNE, mencari pengguna melalui nomor telepon dan LINE ID, atau mendapatkan informasi publik terkait aktivitas pengguna pada layanan LINE lainnya.

Karena informasi pengguna yang dapat diperoleh melalui bot terbatas pada informasi publik dari pengguna yang terdampak (nama tampilan, foto profil, pesan status, dan lain-lain), sehingga tidak ada kebocoran informasi tambahan yang terjadi karena permasalahan ini.

Tindakan kami

Kami sedang melakukan penghapusan atas bot-bot yang mengakibatkan permasalahan tersebut.

Untuk para pengguna yang telah diundang ke banyak grup, kami telah melakukan pembatalan permintaan untuk bergabung ke dalam grup tersebut (*4).

Jika Anda telah bergabung ke dalam suatu grup dimaksud, hal tersebut tidak akan dihapus secara otomatis. Untuk itu kami memohon maaf atas ketidaknyamanannya, dan kami mohon kepada para pengguna yang terdampak untuk meninggalkan grup(-grup) tersebut.

(*4) Jika Anda telah bergabung ke dalam suatu grup tersebut, Anda perlu untuk meninggalkan grup dimaksud secara mandiri.

4. Kronologi Korespondensi

15 Oktober 2020, 17:56: Menerima laporan tentang bug melalui LINE Bug Bounty Program

29 Oktober 2020, 18:15: Menerima laporan pengguna tentang akun CLOVA khusus yang menambahkan pengguna sebagai teman dan mengundang pengguna ke obrolan grup

2 November 2020, 10:38: Dikonfirmasi bahwa API Assistant CLOVA telah digunakan untuk melakukan panggilan dalam jumlah besar

2 November 2020, 16:00: 14 bot yang muncul sebagai akun CLOVA khusus telah dihapus

2 November 2020, 20:30: Patch API Asisten CLOVA pertama didistribusikan

3 November 2020, 13:39: Pemberitahuan tentang gangguan layanan ke layanan Asisten CLOVA diumumkan di Twitter (gangguan terjadi pada 2 November, dari pukul 11:40 sampai dengan pukul 13:51, dan dari pukul 19:18 sampai dengan pukul 22:17).

4 November 2020, 19:00: Gelombang pertama undangan obrolan grup yang dikirim oleh bot dibatalkan

4 November 2020, 20:05: Patch API Asisten CLOVA kedua didistribusikan

5 November 2020, 19:00: Undangan grup chat gelombang kedua yang dikirim oleh bot dibatalkan

16 November 2020, 15:46: Undangan grup chat gelombang ketiga yang dikirim oleh bot dibatalkan

17 November 2020, 19:40: Pemberitahuan dikirimkan kepada para pengguna yang menerima permintaan pertemanan di Jepang, Indonesia, dan wilayah lain melalui Akun Resmi LINE

18 November 2020, 11:35: Pemberitahuan dikirimkan kepada para pengguna di Taiwan melalui Akun Resmi LINE

18 November 2020, 17:30: Pembatalan atas undangan grup obrolan gelombang keempat yang dikirimkan oleh bot

18 November 2020, 20:10: Pemberitahuan dikirimkan kepada para pengguna di Thailand melalui Akun Resmi LINE

20 November 2020, 10:30: Pembatalan atas undangan grup obrolan gelombang kelima yang dikirimkan oleh bot

24 November 2020, 17:42: Pemberitahuan kedua dikirimkan kepada para pengguna yang terkena dampak kejadian ini di Jepang, Taiwan, Indonesia, Thailand dan negara lainnya

5. Terkait laporan bug

Pemberitahuan untuk para peneliti keamanan

LINE telah menerima laporan bug secara rutin melalui LINE Bug Bounty Program sejak tahun 2016 dan memberikan ganjaran yang sesuai dengan peraturan yang berlaku.

Meskipun insiden ini dikaitkan dengan kerentanan yang ditemukan dalam layanan kami, prioritas kami adalah memastikan keamanan pengguna kami dan pengoperasian layanan yang terus berlanjut. Kami memohon pengertian dan kerja sama Anda sehubungan dengan hal-hal berikut

Kami berusaha keras untuk memperbaiki semua kerentanan secepat mungkin Namun demikian, perbaikan dimaksud dapat membutuhkan suatu waktu tergantung dari permasalahannya.

Pada saat melakukan verifikasi suatu kerentanan, mohon untuk menggunakan akun milik Anda sendiri atau mendapatkan persetujuan dari kolaborator yang terpercaya untuk mencegah terjadinya hal-hal yang membahayakan akun pengguna lainnya.

Mohon untuk tidak membagikan informasi kepada pihak lain untuk mencegah terjadinya eksploitasi lebih lanjut sampai dengan kerentanan dimaksud dapat diperbaiki.

Kerentanan yang mengakibatkan spam atau penolakan layanan mungkin membutuhkan waktu lebih lama untuk diperbaiki karena pertimbangan potensi dampak dari tindakan penanggulangan.

Setelah suatu kerentanan ditemukan, mohon segera laporkan bug tersebut ke LINE. Bagian Tindakan Yang Dilarang dalam Ketentuan Penggunaan kami dengan tegas melarang tindakan berbagi, membocorkan, atau mengungkapkan informasi tersebut kepada pihak ketiga atau memverifikasi menggunakan akun lain. Jika terjadi pelanggaran terhadap ketentuan dimaksud, kami berhak untuk menolak pembayaran hadiah dan mengecualikan peserta tersebut dari keikutsertaan dalam LINE Security Bug Bounty Program di masa mendatang. Jika ditemukan adanya suatu pelanggaran, penolakan untuk memverifikasi kerentanan tidak akan berlaku lagi, dan tindakan hukum dapat diterapkan untuk akses yang tidak sah atau penolakan layanan.

Pemberitahuan untuk para pengguna yang telah menemukan suatu kerentanan di LINE

Mohon untuk tidak melakukan tindakan apapun yang dapat merugikan pengguna lain, meskipun informasi mengenai metode tersebut dapat ditemukan dengan bebas. Kami akan mengambil tindakan tegas untuk memastikan bahwa baik pengguna maupun layanan kami tidak terkena dampak negatif. Jika Anda menemukan suatu kerentanan keamanan di LINE, mohon laporkan ke LINE Security Bug Bounty Program. Jika kerentanan tersebut ditemukan oleh orang lain, Anda masih memiliki kesempatan untuk mendapatkan hadiah jika informasi yang Anda sampaikan adalah suatu informasi baru dan dianggap bernilai oleh LINE. Mohon informasikan dalam laporan Anda jika kerentanan dimaksud ditemukan oleh orang lain.

6. Riwayat pembaruan

17 November 2020: Notifikasi dipublikasikan dalam bahasa Jepang, Inggris, Mandarin, dan Bahasa Indonesia.

7. Pertanyaan mengenai kendala ini

Bagi pengguna LINE yang memiliki pertanyaan lebih lanjut mengenai hal ini, silakan menghubungi kami dengan menggunakan tautan di bawah. Harap memilih “Other” pada Pertanyaan #2:

https://contact-cc.line.me/detailId/10666