Exploitatie van de Duolingo API:
Van Massale Notificatiebom tot User Enumeration

Onderzoek naar meerdere kritieke beveiligingslekken binnen Duolingo

Geschreven door:

Maurice Boendermaker

Yassine Abderrazik

Onderzoek uitgevoerd in december 2024

Locatie: Rotterdam, Nederland

Categorie: Cybersecurity / API Exploit Research

Introductie: Kritieke kwetsbaarheid in Duolingo ontdekt

In december 2024 ontdekten Yassine en ik op aanwijzing van een vriend een ernstige kwetsbaarheid in de Duolingo API. Met behulp van een eenvoudig script bleek het mogelijk om massa-notificaties te sturen naar willekeurige gebruikers van de Duolingo-app, zónder dat je ingelogd hoefde te zijn op het betreffende account. De exploit was zo ernstig dat je uit naam van élk willekeurig account (zelfs het officiële account van de CEO, of de Duolingo Admin) meldingen kon verzenden naar élk ander account.

Notificatiebom via onbeveiligde API

Door een kwetsbaar endpoint binnen de Duolingo API konden we iPhone pushmeldingen genereren die direct naar gebruikers werden gestuurd. Deze notificaties konden in grote aantallen verstuurd worden, waarbij het mogelijk was om duizenden meldingen per seconde richting iOS-gebruikers te sturen. De naam van de verzender kon volledig zelf gekozen worden, wat potentieel misbruikt kon worden voor spam, scam of crypto-promotie, iets wat we aantonen met een testaccount met de naam "KOOP NU BITCOIN".

Privacy- en beveiligingsfouten in gebruikersdata

Naast de notificatie-exploit bleek het ook mogelijk om zeer eenvoudig Duolingo user ID’s te achterhalen en daarmee persoonlijke gebruikersinformatie op te vragen via een ander, publiek en verouderd API-endpoint. Hierdoor konden we zien of iemand een betaald abonnement had, welke taaltrainingen iemand volgde, en zelfs in welke tijdzone iemand zich bevond. Sommige privacyinstellingen werden hierbij ook getoond, wat de impact nog groter maakte.

User Enumeration en geautomatiseerd dataverkeer

We bouwden een tweede tool waarmee we via proxies en asynchrone requests in bulk gebruikersinformatie konden ophalen. Dit script maakt gebruik van een reeks roterende IP-adressen en user agents, waarmee de gegevens van tienduizenden Duolingo-gebruikers per sessie konden worden opgehaald. Elk succesvol user ID werd lokaal als JSON-bestand opgeslagen, wat de weg vrijmaakt voor potentiële datamining of scraping op grote schaal.

Mogelijke Premium exploit

Tijdens het onderzoek kregen we ook een mogelijke aanwijzing dat onbeperkte toegang tot Duolingo Premium via een andere API-methode haalbaar zou zijn, zonder betaling. We hebben deze claim echter niet verder getest of geverifieerd, maar het versterkt het beeld dat meerdere beveiligingslagen binnen het platform onvoldoende zijn.

Status van de kwetsbaarheden

Op de dag dat wij van plan waren het notificatielek officieel te melden bij Duolingo, bleek het probleem precies die dag verholpen te zijn. Het is dus niet langer mogelijk om meldingen vanuit en naar willekeurige accounts te sturen. De user enumeration kwetsbaarheid, waarbij gebruikersdata zoals tijdzone, cursussen en abonnementstatus eenvoudig opvraagbaar zijn, is echter op het moment van schrijven nog steeds actief en onbeveiligd.

Verantwoord Disclosure Disclaimer

Bij het ontdekken van deze kwetsbaarheden hadden wij de intentie om deze op verantwoorde wijze te melden aan Duolingo. Via de daarvoor bestemde route op https://www.duolingo.com/.well-known/security.txt wilden wij contact opnemen met het officiële security e-mailadres: security@duolingo.com.

Op de dag dat wij onze melding wilden indienen, bleek het kritieke notificatielek echter al te zijn verholpen. De user enumeration-kwetsbaarheid is op het moment van schrijven nog actief.

We hopen dat dit rapport bijdraagt aan het bewustzijn en de verbetering van de beveiliging van grootschalige platforms zoals Duolingo.

Contactgegevens

Maurice Boendermaker
maurice@monadius.com
https://mauriceb.nl

Yassine Abderrazik
yassinabde@outlook.com