Exploits in the Duolingo API:
From Mass Notification Bomb to User Enumeration

Investigation into multiple critical security vulnerabilities within Duolingo

Written by:

Maurice Boendermaker

Yassine Abderrazik

Investigation conducted in December 2024

Location: Rotterdam, Netherlands

Category: Cybersecurity / API Exploit Research

Introduction: Critical Vulnerability Discovered in Duolingo

In December 2024, Yassine and I discovered a serious vulnerability in the Duolingo API at the suggestion of a friend. Using a simple script, it was possible to send mass notifications to random users of the Duolingo app, without having to be logged into the account in question. The exploit was so serious that you could send notifications on behalf of any account (even the official account of the CEO, or the Duolingo Admin) to any other account.

Notification bomb via unsecured API

A vulnerable endpoint within the Duolingo API allowed us to generate iPhone push notifications that were sent directly to users. These notifications could be sent in bulk, potentially sending thousands of notifications per second to iOS users. The sender name could be completely customized, which could potentially be abused for spam, scams, or crypto promotion, which we demonstrate using a test account named "BUY BITCOIN NOW".

Privacy and security flaws in user data

In addition to the notification exploit, it was also possible to very easily obtain Duolingo user IDs and thereby retrieve personal user information via a different, public and outdated API endpoint. This allowed us to see if someone had a paid subscription, which language courses they were taking, and even what time zone they were in. Some privacy settings were also exposed, which made the impact even greater.

User Enumeration and automated data traffic

We built a second tool that allowed us to retrieve user information in bulk via proxies and asynchronous requests. This script used a series of rotating IP addresses and user agents, allowing it to retrieve data from tens of thousands of Duolingo users per session. Each successful user ID was stored locally as a JSON file, paving the way for potential data mining or scraping at scale.

Possible Premium exploit

During our investigation, we also received a possible indication that unlimited access to Duolingo Premium might be achievable via another API method, without payment. We did not test or verify this claim further, but it reinforces the idea that multiple layers of security within the platform are insufficient.

Status of the vulnerabilities

On the day we planned to officially report the notification leak to Duolingo, the problem was fixed that very day. It is no longer possible to send notifications to and from arbitrary accounts. However, the user enumeration vulnerability, which allows user data such as timezone, courses, and subscription status to be easily retrieved, is still active and unsecured at the time of writing.

Responsible Disclosure Disclaimer

When we discovered these vulnerabilities, we intended to report them responsibly to Duolingo. We wanted to contact the official security email address: security@duolingo.com via the designated route at https://www.duolingo.com/.well-known/security.txt .

However, on the day we wanted to submit our report, the critical notification leak had already been fixed. The user enumeration vulnerability is still active at the time of writing.

We hope that this report will contribute to raising awareness and improving the security of large-scale platforms like Duolingo.

Contact details

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

Yassine Abderrazik
yassinabde@outlook.com