Intercode GraphQL cross-domain security issue postmortem

Postmortem Owner: Nat Budin
Attendees: Nat Budin, Dave Kapell, Marleigh Norton, Jaelen Hartwin
Meeting Scheduled For: Saturday, January 8, 2022, 10:00 AM PST

Overview

In the course of upgrading Intercode to Rails 7, Nat discovered a major security issue that has been in the app pretty much since the beginning. The issue revolved around the “become user” feature. It allowed a user with access to the "become user" feature in any convention to use direct GraphQL API calls to act as that user across conventions. This issue has now been fixed, but was present in Intercode 2 since its rollout. We do not believe that this issue was ever exploited, but cannot conclusively prove that.

How did we discover this issue?

Rails 7 adds a security feature that prevents accidental open redirects in applications. In order to do this upgrade, we had to audit all existing redirects in Intercode to make sure this feature wouldn't break them. While doing so, we realized that the existing redirect intended to prevent using "become user" to access a different convention only worked within the UI, and wasn't triggered via direct API calls.

Contributing Factors

- "Become User" feature is powerful and hard to reason about
- Intercode is functionally a single-developer project
- QA is mostly done via click-testing, which wouldn't have allowed this exploit
- We made the decision to import all past Intercon and Concentral conventions, which dramatically increased the number of users with "become user" permissions in a hosted con
- Log retention for the entire lifespan of this app would have been cost-prohibitive for NEIL, so we can't conclusively prove that this was never exploited

Resolution

1. Added a unit test method for consistently testing that cross-domain "become user" doesn't work, while same-domain "become user" does.

2. Applied this method across all privilege assertions in our unit test suite.
3. Fixed any resulting test failures.
4. Deployed this code change to production, and notified Consequences UK to update their instance of Intercode ASAP.

Impact

We have no way of proving for sure whether or not this bug was ever actually exploited. There have been no reports of anything that seems like this kind of privilege escalation.

The only people who could have exploited this bug are semi-trusted users who have admin privileges in at least one hosted convention site. There are 105 such users.

If the bug was exploited, it would have been possible for an attacker to do the following things across all hosted convention sites. (Since the attacker would have to be an admin at some convention, these are things they could already legitimately do in that convention.)

- Read and modify private contact information for other users
- Read and modify event signup lists
- Read and modify event scheduling and descriptions
- Read and modify convention-specific settings, including signup schedule, pricing, event categories, proposal forms, and other settings

This bug did NOT allow an attacker to:

- Read or modify authentication information
    - *We never store plaintext passwords*
    - *The "become user" permission has never allowed users to access the underlying user account (login email and password)*
- Read or modify payment methods
    - *We never handle payment details; these are sent directly to our payment processing platform (Stripe) and never touch NEIL servers*

Timeline

Time (UTC)	Event
12/23/2021	Nat discovers issue and discloses to Dave (NEIL Hosting co-coordinator)
12/28/2021	Fix rolled out

12/28/2021	Disclosure to Consequences admins with a request to apply patch

How'd We Do?

What Went Well?

- We discovered the issue ourselves
- We had a fix out to production within a week of discovery (and that week included Christmas)
- The existing design of the system ensured that payment data and login data couldn't be compromised via this exploit
- We had an existing set of comprehensive unit tests on the permission system, and having that in place made it easier to fix this
- Intercode automatically notifies convention staff of modifications to events and event proposals, which gives us some confidence that this bug wasn't used to do that

What Didn't Go So Well?

- It took approximately 4 years for this bug to be discovered
- We have no way to prove that it wasn't exploited (though we don't believe it was)
- This bug granted extremely wide-ranging access

Action Items

- Add a logging mechanism for actions taken in "become user" sessions, add a "justification" field when someone becomes a user (recorded with timestamp)
    - Now deployed to production: https://github.com/neinteractiveliterature/intercode/pull/6106
- Turn on the free PaperTrail log retention (10MB/day, 7 days) to see how much logs we're actually generating
    - Done, awaiting results
    - We definitely don't fit in the free option. We're generating around 20MB/day. The next tier up is $8/month which is feasible but let's also evaluate other options
    - Disabling in favor of AWS CloudWatch, see below
- Evaluate log retention options and see if longer log retention would be feasible
    - Trying out AWS CloudWatch logging; I think we fit in the free tier but even if we don't, it would probably cost around $0.50/month. Whether it's as usable as PaperTrail is an open question
    - Usability is frankly not as great as PaperTrail but it's perfectly livable, and very much looks like we will never exceed the free tier. Additionally, we can log in

JSON format and it has a really sophisticated query syntax we can use to filter JSON logs, which is a plus
    - Going with CloudWatch going forward. Leaving it at 1 month retention for the moment but will re-evaluate after a few months and see if we could increase it

Messaging

Hey all. This thing happened we should tell you about.

While performing platform upgrades, we found a bug in Intercode, the website code used by conventions such as Intercon. It has since been fixed.

This bug created an exploit where people with leadership access to one Intercode convention could use certain permissions on any convention. As a reminder, not even admins have access to your passwords or financial information.

Due to the technical complexity of accessing the exploit and the small number of people who had the permissions required to take advantage of this, we don't think it was used, but can't prove it.

What Happened?

It's technically possible con leadership from one convention looked at or modified information for conventions they should not have had access to. We don't think anyone did, and it's since been fixed, but here's the low down.

There's a function called *"Become user"* which certain people on the convention team have permissions for. Just like it sounds, it lets people see the convention website as if they were logged in as the selected user. It's used for things like running the convention, debugging, and accessing the website on behalf of a user at their request. It does not allow access to anyone's passwords or payment information.

This permission is fairly restricted and convention specific. That being said, if you had *Become user* permissions on one convention using Intercode, it turns out there was a way to then *Become user* on any Intercode convention. It would involve coding and would not be easy, but it was possible. For example, someone with admin access to Intercon S could have accessed admin functions on Be-Con 2019, including viewing and modifying event and attendee data.

What Are We Doing About This?

The bug has been fixed and the exploit is gone. We've also reviewed the list of people who have *Become user* permissions on any Intercode site. Considering the difficulty of finding the exploit, the technical expertise required to use it, and the limited set of people who have the necessary permissions, we think it's really unlikely anyone did so. That being said, we can't prove a negative.

A post-mortem was held to document the exploit, which you can find at
Intercode GraphQL cross-domain security issue postmortem
It includes timelines and technical details for the interested.

And of course, we're now telling you about it. We take the safety and security of our community very seriously, which means owning up to our mistakes. We apologize this happened at all, and we're even more sorry it took us so long to notice it.

Thanks for your faith in us.

The Intercode Team
Nat Budin (he/him)
Dave Kapell (he/him)
Jae Hartwin (they/them)
Marleigh Norton (she/her)