Preliminary report: November 2026 security incident

On 9 and 10 November 2026, an unauthorized third party accessed parts of Apify's internal network and used that access to read customer account records, sessions, and API tokens. For a small subset of active accounts, it also read some stored data. The unauthorized third party’s network path into our internal systems was closed on 10 November. The credentials it had already stolen continued to work until we rotated them on 11 and 12 November.

This report is preliminary. Our investigation is ongoing, and some details may change. We have notified the Czech National Cyber and Information Security Agency, the Office for Personal Data Protection, and the police.

A full incident report, including the root cause and completed remediation, will follow once all activities are complete.

What happened

The unauthorized third party started with a set of working Apify API tokens, including a token belonging to an Apify staff member with higher privileges.

With the staff API token, the unauthorized third party used a previously unknown vulnerability in one of our networking services to access our internal network. There, it reached an internal cache that held sessions. Using sessions taken from the cache, including sessions of Apify staff with higher privileges, it read account records in bulk through our internal admin tools.

On 10 November, an Apify engineer reported an unrelated vulnerability. While fixing it, we tightened network rules, which closed the unauthorized third party's path into the internal network. We were not aware of the incident at that point, but additional log analyses identified the unauthorized third party's activity, and we started incident response.

When (UTC)	What happened
9 Nov, 10:00	First unauthorized activity: password guessing, registration of OAuth apps, probing of public endpoints. None of the activities succeeded.

When (UTC)	What happened
9 Nov, 12:00	The unauthorized third party uses a staff token, gets into our internal network and reaches an internal cache holding sessions.
10 Nov, 18:00	Network rules tightened. The path into the internal network is closed.
11 Nov, 12:00	Additional log analyses identify the unauthorized third party's activity. Incident response starts.
11–12 Nov	All sessions ended, credentials of affected accounts rotated and affected customers notified

Scale of impact

We traced the unauthorized third party's requests through our audit logs. Every affected account owner has received an email describing the impact on their account. We distinguish between multiple categories:

- Access tokens
- Account data
- Customer data

If you haven't received one, we have not identified your account as affected. You can reply to the emails with additional questions. We are doing our best to reply to all inquiries as soon as possible.

What was not exposed

- **Secret Actor input fields and secret environment variables.** They are stored encrypted and can only be decrypted on the servers that use them. They were not exposed.
- **Passwords.** Apify never stores account passwords in plain text, so they were not exposed in plaintext. Apify uses salted bcrypt.
- **Full card numbers.** Apify never stores them.

What you should do

All these relevant activities were shared with affected users, and unless you did, please proceed with the relevant activities:

1. **If you got an email from us, follow its instructions.** If you haven't, we have not identified your account as affected. If our email told you that your authentication data (including your hashed password) was accessed, we recommend updating your password as a precaution.
2. **Set General resource access to Restricted** (Console → Settings → Login & Privacy > **General resource access**). While it is open, anyone who knows a storage ID can read that storage. This is the default for every new account since April 2026 and is our recommended setting.
3. **Reconnect your integrations** when prompted (Zapier, n8n, Make, and others), as we have proactively rotated all OAuth secrets as a precaution.
4. **Reconnect GitHub** if you build Actors from private repositories: open an Actor source tab→ Change provider → GitHub → authorize.
5. **Use new API tokens.** We rotated the tokens for affected accounts. All tokens are hashed now, so they are not retrievable anymore using the Apify Console UI.
6. **Set up 2FA again** if we asked you to or if you do not have 2FA active yet.
7. **Watch for phishing** attempts that use your account details. Apify will never ask for your password, 2FA codes, or payment details.

What we have done

We identified the attack vector and hardened the setup at multiple layers. Each of these measures significantly reduces the risk of a similar incident or limits its potential impact. We also identified further changes that should decrease the impact of potential incidents in the future. Below are the main ones we are sharing now.

Some measures are not listed here for security reasons, and we will provide more details in our final report with additional reasoning.

- Preventively ended all Apify Console sessions.
- Rotated API tokens and proxy passwords for affected accounts without advance notice because the unauthorized third party held working copies. We are aware that this broke production jobs for some of you, and we’re sorry for the disruption it caused but it was necessary to prevent further unauthorized access.

- Revoked GitHub connections, and as a precaution, we rotated OAuth credentials with the respective integration partners.
- Store API tokens and session keys only as hashes.
- Hash or encrypt proxy passwords, 2FA secrets, and recovery codes.
- Implemented additional controls in internal networking to minimize the blast radius of a similar incident.
- Added network-level restrictions for internal tools on top of existing authentication.
- Extended monitoring of our logs for suspicious activity to speed up detection of similar incidents and increase coverage.
- Started an additional security review of our code and infrastructure with external scanning tools and are hardening across multiple security layers.

FAQ

Did the unauthorized third party change anything in my account?
We found objects the unauthorized third party created in a few accounts: webhooks, Actors, and one edited schedule. These were attempts to reach our internal network, not to cause individual damage. We backed them up, removed them, and contacted the owners.

Was my plain-text password exposed?
We never store plain-text account passwords. For accounts whose full records were read, the salted bcrypt hash of the password was also read.

Is my 2FA still safe?
For accounts whose full records were read, the 2FA secret and recovery codes were read. We emailed those users to set up 2FA again.

Were my private GitHub repositories accessed?
GitHub connection tokens were in the cache. We revoked all of them on 11 November at 14:20 UTC, which also removed the deploy keys. We have no sign they were used. However, we recommend checking on your end (https://github.com/settings/security-log).

What about my payment card?
For accounts whose record was read and had a payment card on file: last four digits, expiry date and cardholder name. Full card numbers are never stored by Apify.

Why did my integration, scheduled job or proxy stop working?
Because we rotated your token, proxy password or integration connection. Update the token in your systems or reconnect the integration.

Is the unauthorized third party still active?
We have not detected malicious activity from the unauthorized third party since 12 November.

Who is behind this, and what did they want?
We don't know who is behind the incident. The activity was mostly reading account data and, for a subset of accounts, stored data.