Incident Report for Jan 10th

https://resend.com/blog/incident-report-for-january-10-2024

Summary (TL;DR)

On January 7th, attackers used a leaked environment variable of the Resend database API to access customer data including Emails Sent, Domains, API Keys (encrypted), Logs, and Contacts, affecting all users.

The actual content of the emails was not accessed, nor were any unencrypted private keys for the Resend API or DKIM. No user action is required to continue safely sending.

We have since closed the access and rotated all database keys. Additionally, we are partnering with third-party cybersecurity company, Oneleet, to conduct an exhaustive investigation and help us ensure this attack cannot occur again.

We are deeply sorry for the impact this had on our users. We remain committed to transparency and prevention. The following is a summary of what went wrong, how the incident was resolved, and the work we are doing to ensure it does not happen again.

Incident timeline

All timestamps referenced are in Coordinated Universal Time (UTC).

- On December 30th, at 11:20 pm, the attackers first gained access to our system by discovering an exposed database API key as an environment variable on the client-side of the Resend Dashboard.
- On December 31st, at 12:28 pm, a Resend team member discovered that multiple users were sharing the same billing information. This appeared to be a strange bug and did not raise enough of a red flag during the holiday weekend for further investigation. An alarm was put in place to make sure this didn't happen to other users.
- On January 7th, at 7:28 pm, the attacker started accessing data.
- On January 9th, at 4:47 am, a user was discovered to have unblocked email sending on their account. During normal operations, senders are blocked for not complying with our

Acceptable Use Policy. One of these users was able to update fields normally not accessible to users in order to unblock their sending. With further investigation, it appears they had already done this three times.

- On January 9th, at 4:59 am, this incident was promoted to SEV-0 internally. We understood this attack to be a form of hijacking of an existing API request, not accessing the database.
- On January 9th, at 5:21 pm, logs were discovered showing GET, PATCH, and DELETE requests to the database, making it clear that the database API layer had been accessed, but not clear the full exposure.
- On January 9th, at 11:01 pm, logs were discovered showing programmatic access of database tables, which allowed us to establish the method, extent, and severity of the access. Our audit of the entire database leads us to be confident that we know the impact of the incident and have comprehensive knowledge of what happened and what steps we need to take to remediate this.
- On January 10, at 2:32 am, the remediation was deployed to production.
- On January 10, at 3:21 am, the database credentials were rotated, causing a 25 minute downtime.

How this affects you

No user action is required to continue safely sending. You may consider consulting an attorney regarding data privacy implications in your jurisdiction.

If you need an export of your data, please contact us at security@resend.com.

Here is a comprehensive list of what data was impacted. Only data after November 1st, 2023 was accessed.

Emails Sent

- Accessed: Recipient address, sender address, sent date, subject, bcc, cc, reply to, and last event.
- Not Accessed: No email content body which includes the HTML and plain text.

Domains

- Accessed: Domain names, verification status, region, and DKIM public keys.
- Not Accessed: No unencrypted DKIM private keys.

API Keys

- Accessed: Names, permission roles, and encrypted tokens.
- Not Accessed: No unencrypted tokens.

Logs

- Accessed: HTTP Response data such as status code, and HTTP Request data such as method, and endpoint.
- Not Accessed: No HTTP Response JSON body, and Request JSON body, or headers.

Contacts

- Accessed: Email addresses and names.

Users

- Accessed: Resend user email addresses.
- Not Accessed: No Resend user names or passwords.

Actions and remediations

These are the preventative measures that **we have already taken**:

- Removed database API environment variable from the client-side of the Resend Dashboard.
- Rotated database API access keys.
- Enforced MFA across all systems touching the database.
- Conducted org-wide password reset across all systems touching the database.

These are the preventative measures that we **will be taking immediately**:

- Improving monitoring and alerting for database API access.
- Partnering with a third-party cybersecurity company, Oneleet, to conduct an exhaustive investigation.

Please reach out to us at security@resend.com if you have any questions.

Conclusion

We sincerely apologize to everyone affected by this incident, and we appreciate your understanding as we learn to navigate this challenging period.

This has been an unfortunate and trying moment for us, but solidified the determination and commitment of each and every team member at Resend.

Your trust is what has built us, and we remain deeply committed to ensuring your sending is safe.