

INTELLIGENCE BRIEF

The Fireworks AI Breach Makes AI Vendors a Third-party Risk Tier

Stolen Fireworks AI credentials and an exposed access key reached customer data at Uber, Notion and Cursor. Inventory AI vendors and keys, minimize what you send, and rotate secrets when a vendor reports a breach.

EDITION

Fall/Winter 2026/2027 Edition

BA-02 · Breach analysis

PUBLISHED BY

Z7 Solutions LLC

Orlando, Florida

READ ONLINE

z7solutions.com

844-974-8669

01 At a Glance

STATUS

ONGOING RISK

Fireworks' November 17 bulletin calls both October incidents contained and remediated, while Notion says its own investigation is continuing. [1]

HEADLINE NUMBERS

149,346
Uber drivers notified, per reported state filing [5]

5,000
Most Cursor users who received the tampered extension [2]

<1%
Notion workspaces affected [3]

2
Separate Fireworks incidents in October [1]

KEY FACTS

VENDOR
Fireworks AI, an inference and model hosting provider [1]

FIREWORKS INCIDENTS
Two separate incidents in October 2026 [1]

UBER
Driver data; 149,346 people notified per state filing reporting [4]

CURSOR
Exposed access key; at most 5,000 users received a tampered extension [2]

NOTION
Fewer than 1% of workspaces; some AI chat transcripts [3]

FIREWORKS ATTRIBUTION
A financially motivated group tied to selling LLM tokens [1]

02 What Happened

Fireworks AI disclosed two separate security incidents in October 2026. Customers Cursor, Notion and Uber each reported consequences tied to the Fireworks compromise. [1, 2, 3, 4]

- Fireworks says it identified unauthorized use of internal credentials on October 6. The attacker reached environment variables in evaluation jobs for a limited number of customer accounts, including API keys and tokens stored as secrets. [1]
- A second incident ran from October 23 to October 30. Fireworks says an attacker reached development machines hosted by a third-party cloud provider, then part of production, and accessed account and billing information for all accounts created before October 30. [1]
- Cursor says an access key it had issued to Fireworks was obtained by an attacker, who copied data from a read-only storage bucket shared with Fireworks. A tampered extension was then available for approximately 11 hours, reaching at most 5,000 users. [2, 6]
- Notion says Fireworks notified it of an incident affecting fewer than 1% of workspaces, involving unattributable AI chat sessions. Notion disconnected from Fireworks as of November 3 and found that data was retained from the Fireworks endpoints it used. [3]
- Uber's letter says a service provider notified it on October 9 that its internal credentials were compromised and used to reach Uber's account with that provider. Press identified the provider as Fireworks and reported nearly 150,000 drivers notified. [4, 5]

03 How It Works

01 Steal vendor credentials

Fireworks reports that stolen internal credentials, and later a compromised third-party cloud provider, gave the attacker a way into its systems. [1]

02 Reach secrets and shared storage

Fireworks says customer secrets such as API keys and tokens were captured in some accounts. Cursor says a key it issued to Fireworks opened a shared storage bucket. [1, 2]

03 Use secrets against customers

SecurityWeek reports the bucket contained unredacted credentials that opened SaaS tools used by Cursor. Uber's letter says the vendor's credentials were used to access Uber's account with the vendor. [4, 6]

04 Abuse trusted distribution

Cursor says the attacker published tampered copies of a Claude Code extension that were not present in the Open VSX marketplace source. Uninstalling alone may not be enough. [2, 6]

05 Monetize LLM access

Fireworks links the activity to a financially motivated group that sells LLM tokens obtained through unauthorized access to illicit routing gateways. [1]

04 Who Is at Risk

Any organization that sends prompts, files, datasets or credentials to an AI inference or model hosting provider inherits that provider's security.

- Customers whose API keys, tokens or other secrets are stored in a vendor platform, since Fireworks says removing a stored secret does not invalidate the underlying credential. [1]
- Organizations that rely on a contractual zero data retention promise without testing it, since Notion found data retained from the endpoints it used. [3]
- Employers and platforms holding personal data that a vendor can reach, as the Uber notices show. [4]
- Developer teams that install tools through extension marketplaces and issue shared keys to partners. [2]

Sectors in scope: Organizations sending data to AI inference and model hosting providers, Software and AI product companies with vendor-held data, Employers and platforms whose personal data sits with a service provider.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 November 9: Fireworks widened its disclosure to resource metadata, billing information and, for certain customers, a subset of incomplete model weights and datasets. It said payment card numbers are not stored by Fireworks.

SOURCE 1

02 November 17: Fireworks stated that the earlier and later activity are two separate incidents and that both are contained and remediated.

SOURCE 1

03 Cursor moved all inference traffic off Fireworks, deactivated the key it had issued and rotated every exposed credential it found.

SOURCE 2

04 Notion disconnected from Fireworks, disabled its Insights feature during the investigation and announced an audit of critical vendors for data minimization and zero data retention practices.

SOURCE 3

05 Week of November 16: Uber's driver notices and state filings put a count on the downstream personal data exposure.

SOURCE 5

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Inventory every AI vendor and every API key, token and connector that reaches one.**

You cannot rotate or cut off access you cannot list; Fireworks customers needed to find and replace keys quickly. [1]

02 **Scope each key to one purpose, set an owner and expiry, and rotate on a schedule.**

Narrow, short-lived keys limit what a vendor-side theft can open; Cursor's single issued key reached a shared bucket. [2]

03 **When a vendor reports a breach, rotate third-party credentials at the issuer, not only inside the vendor platform.**

Fireworks warns that removing a stored secret alone does not invalidate the underlying credential. [1]

04 **Minimize what you send to inference providers and keep secrets and personal data out of prompts.**

Notion's guidance tells users to keep secrets out of chats and documents, and its transcripts included whatever users typed. [3]

05 Verify zero data retention claims with the vendor and by testing, and check what each feature stores.

Notion learned that data was retained from the Fireworks endpoints it used, and its commitment does not cover stored-history features. [3]

06 Add breach notification timelines and subprocessor disclosure to AI vendor contracts.

Uber learned of the compromise from its provider on October 9, and Uber said it had alerts enabled but none triggered. [4, 5]

07 Log vendor API use and alert on unfamiliar keys, users, jobs, datasets and unusual traffic.

Fireworks and Notion both advise reviewing audit and access logs for unrecognized activity. [1, 3]

08 Write an offboarding runbook that disconnects data flows, revokes keys and confirms deletion.

Uber severed data connections, Cursor deactivated its key and Notion disconnected and reported data deleted from Fireworks systems. [2, 3, 4] If you want help with this, Z7 offers vendor risk review and Managed Private AI (/ai-services/managed-private-ai/) for keeping inference data under your control.

07 Sources

[1] **Fireworks security bulletins (October 10, November 9 and November 17, 2026)** Fireworks AI · October 10, November 9 and November 17, 2026. https://fireworks.ai/security-bulletins

[2] **Security incident update** Cursor · As published by Cursor, November 2026. https://cursor.com/blog/security-incident-update

[3] **Notice about the Fireworks AI incident that may impact some Notion workspaces** Notion · November 2026. https://notion.com/help/security-incident-involving-a-third-party-ai-vendor

[4] **Uber notifies drivers of data breach affecting nearly 150,000 people** BleepingComputer · November 2026. https://www.bleepingcomputer.com/news/security/uber-notifies-drivers-of-data-breach-affecting-nearly-150-000-people/

[5] **Uber confirms hackers stole thousands of drivers' license information in data breach** TechCrunch · November 16, 2026. https://techcrunch.com/2026/11/16/uber-confirms-hackers-stole-thousands-of-drivers-license-information-in-data-breach/

[6] **Cursor Supply Chain Attack Started at Fireworks AI** SecurityWeek · November 16, 2026. https://www.securityweek.com/cursor-supply-chain-attack-started-at-fireworks/

NEXT STEP

What does this mean for your security?

Bring your questions about Fireworks AI, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

- SitusAMC breach settlement and vendor risk
  More from the edition · z7solutions.com/z7-cyber/situs/
- OAuth data theft can outlast a password reset
  More from the edition · z7solutions.com/z7-cyber/saas-oauth-data-theft/
- Qilin still tops most ransomware counts
  More from the edition · z7solutions.com/z7-cyber/qilin/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A SECURITY CONVERSATION Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.