The right model for every task. Try Nexus

← All security bulletins

Security bulletin

Fireworks October 2026 security incident

Last updated October 10, 2026, 11:16 PDT Active monitoring

On this page

Who is affected?

What we know

What was affected?

What we have done

What affected customers should do

Contact

On October 6, Fireworks identified a security incident involving unauthorized use of internal Fireworks credentials. An unauthorized third party accessed environment variables used in evaluation jobs in a limited number of customer accounts. Based on our investigation at this time, we have not detected evidence of unauthorized access to customer models, datasets, training data, personal information, or inference traffic within the Fireworks security perimeter or control.

We began containment the same day and have directly notified every identified affected customer. We are actively monitoring for further activity. We recognize the concern and work this creates for affected customers, and we are providing account-specific information to help them respond.

We're working with a cybersecurity expert firm to assist with the incident.

Who is affected?

The incident affected a limited number of customer accounts. Affected customers received a direct email identifying the credentials requiring action.

If you have not received a notice, we have not identified your account as affected based on our investigation to date. If that changes, we will contact you directly.

What we know

The following timeline records our findings, response actions, and ongoing updates (PDT):

Date, PDT	Finding or action
Oct 6 9am, 2026	Fireworks identified the activity and began containment.
Oct 7 7am, 2026	Started notifying affected customers
Oct 9 4pm, 2026	Rotated Fireworks employee API keys
Oct 9 6pm, 2026	Notified identified affected customers
Oct 9 10pm, 2026	Published bulletin
Oct 10, 2026	Revoked additional Fireworks user API keys and rotated service-account tokens identified in a completed credential review. Further credential review and rotation are continuing.

What was affected?

We believe that environment variables, including API keys and tokens stored as secrets, were captured in certain affected accounts. Based on our investigation at this time, we have not detected evidence of unauthorized access to customer models, datasets, training data, inference traffic (including prompts and outputs), or personal information within the Fireworks security perimeter or control. Fireworks does not store prompts or outputs by default, as our platform is ZDR. We are continuing to review calls made with the exposed credentials to verify the scope, and our review of other potential access remains ongoing.

What we have done

We have revoked identified internal credentials used in the incident, affected Fireworks API keys, and keys identified as created by the actor, and added access restrictions. We are actively monitoring for further activity.

We are also reviewing how secrets are made available to evaluation jobs. We will share additional remediation measures as they are implemented and verified.

What affected customers should do

1. **Replace revoked Fireworks API keys if you still need them.** The Fireworks API keys identified as revoked in your notice no longer work. Create new keys in your Fireworks account and update the applications that used the revoked keys. Those applications will fail authentication until updated.

2. **Rotate third-party credentials identified in your notice.** Rotate or revoke them with the providers that issued them, then update the applications and Fireworks secrets that use them. Removing a stored secret alone does not invalidate the underlying credential. Third-party credentials require action with their issuing providers.

3. **Review data and activity associated with exposed third-party credentials.** If your notice identifies third-party credentials, work with those providers to review access logs and data accessible using those credentials, including for unauthorized reads, downloads, or changes. Rotate the identified credentials even if you do not find suspicious activity, and follow the provider's guidance if you identify unauthorized access.

4. **Check for unrecognized resources or activity.** Review API keys, users, evaluators, training jobs, and datasets. Send us the names or IDs of anything you do not recognize so we can determine whether it is related and help you address it.

We can provide secret names and credential fingerprints through a secure channel to help you identify the exact credentials requiring rotation.

If you have not received an affected-customer notice, no incident-specific action is currently required. Contact us if you observe suspicious activity or need help confirming your account's status.

Contact

Reply to your incident notification email or contact security@fireworks.ai.

✓ SOC 2 Type 2 ✓ ISO 27001 ✓ ISO 27701 ✓ ISO 42001

Products Solutions

Overview
Inference
Nexus
Training
Sovereign
Pricing

For enterprise
For startups
Code assistance
Conversational AI
Agentic systems
Search
Multimodal
Enterprise RAG

Partners

AMD
AWS
Microsoft
NVIDIA

Developers

Community
Model library
Docs
Cookbooks
Changelog
API
Status page

Resources

Customers
Blog
Events

Company

About
Careers
Newsroom
Trust center
Contact sales

Fireworks

© 2026 FIREWORKS AI, INC.