The right model for every task. Try Nexus

← All security bulletins

Security bulletin

Update on October 2026 security incident

Last updated November 9, 2026 Active monitoring

On this page

The update

Further activity

Data involved

What we have done

Contact

The update

This is an update to our previous security bulletin published on October 9, 2026. In response to the incident, we notified law enforcement and obtained assistance from a leading cybersecurity firm, Palo Alto Networks Unit 42, to help conduct forensic analysis. At the time of publishing the bulletin, only Fireworks stored secrets (e.g. used in evaluation jobs) were known to have been accessed. Since then, we discovered impacts to account and billing information. For a limited set of accounts, we also discovered impact to secrets, datasets, and incomplete models.

The evidence indicates links to a cybercriminal threat actor group, which is financially motivated and aimed at selling tokens from unauthorized access to Large Language Models (LLMs) to illicit routing gateways, known as "LLMJacking". On November 2, Google Threat Intelligence Group and Mandiant published a blog post about the rise of LLMJacking, their motives, techniques used, and mitigation.

Further activity

A third-party cloud provider that hosted Fireworks R&D machines experienced a security incident on October 23. On October 24, the unauthorized third party used it to reach Fireworks development machines and then run an unauthorized workload that led to additional customer data impact. We detected this activity on the same day, and followed our incident response processes to take immediate remediation measures and close known critical vulnerabilities. As of October 25, we have not detected further evidence of successful unauthorized access by the threat actor on the Fireworks platform customers use.

Data involved

The affected internal application provided access to the following categories of information:

- **Resource metadata**, such as Fireworks resource identifiers, display names, descriptions, creation time, etc.
- **Billing information**, such as billing and shipping addresses, invoice and payment history, account balance, and credit usage. Payment card numbers are not stored by Fireworks and were not impacted.
- **Model weights and datasets**, for certain customers, a subset of incomplete model weights and datasets were accessed.

We are notifying customers whose data was impacted, and providing details about the impact and recommended response actions.

We have not detected any impact to Inference, Training SDK and Nexus, which are all zero data retention (ZDR) by default. These findings are based on our investigation to date. Our investigation is ongoing and may reveal additional information.

What we have done

Working with Unit 42, Fireworks identified and implemented security hardening procedures, including:

- **Access and credential lockdown**. Fireworks revoked and replaced credentials and service accounts, removed unnecessary elevated privileges, and tightened controls designed to prevent new unauthorized credentials from being created.
- **Network isolation**. Fireworks restricted unauthorized network pathways and isolated affected systems designed to prevent further unauthorized activity and movement between systems.
- **Data protection**. Fireworks reviewed and tightened access to data storage and analytics systems and enforced controls designed to prevent public or unauthorized access to stored data.
- **Forensic and audit integrity**. Fireworks secured and enhanced our logging and monitoring systems.

As part of our response, we've disabled self-serve dataset uploads and downloads used by Batch Inference and dataset-based training while we investigate this incident. Training SDK remains available with ZDR, i.e. no training data stored at rest, and Fireworks Lab-based training operates in an isolated environment with additional network and storage protection. We continue to work with Palo Alto Networks Unit 42 on our investigation and security hardening.

We will continue to monitor our systems 24/7 and will provide further updates on our investigation as appropriate.

Contact

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

SOC 2 Type 2 ISO 27001 ISO 27701 ISO 42001

Products

Overview
Inference
Nexus
Training
Sovereign
Pricing

Solutions

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

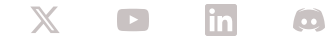
About

Careers

Newsroom

Trust center

Contact sales



© 2026 FIREWORKS AI, INC.

Privacy policy Terms of service Security bulletins Privacy choices