
Gemini AI Data Exposed **2,800+ Keys Found Leaked Online**

Gemini AI Data Exposed

A dangerous security gap has quietly persisted for years, suddenly becoming critical with the introduction of Generative AI. Researchers have discovered nearly three thousand Google API keys exposed in public-facing website code, many belonging to major financial institutions, security companies, and even Google itself. These keys, originally designed as non-sensitive identifiers for services like Maps and YouTube embeds, now serve as authentication credentials for Google's Gemini AI assistant, giving anyone who finds them access to private data and the ability to rack up massive usage charges.

API Keys That Gained New Privileges

Before Gemini, Google Cloud API keys were considered relatively low-risk. Developers embedded them in client-side code for legitimate purposes:

- Loading Google Maps on a website.
- Embedding YouTube videos.
- Tracking usage with Firebase.
- Authenticating for various Google services.

Because these keys were designed as identifiers rather than sensitive credentials, their exposure in page source code was not considered a critical vulnerability.

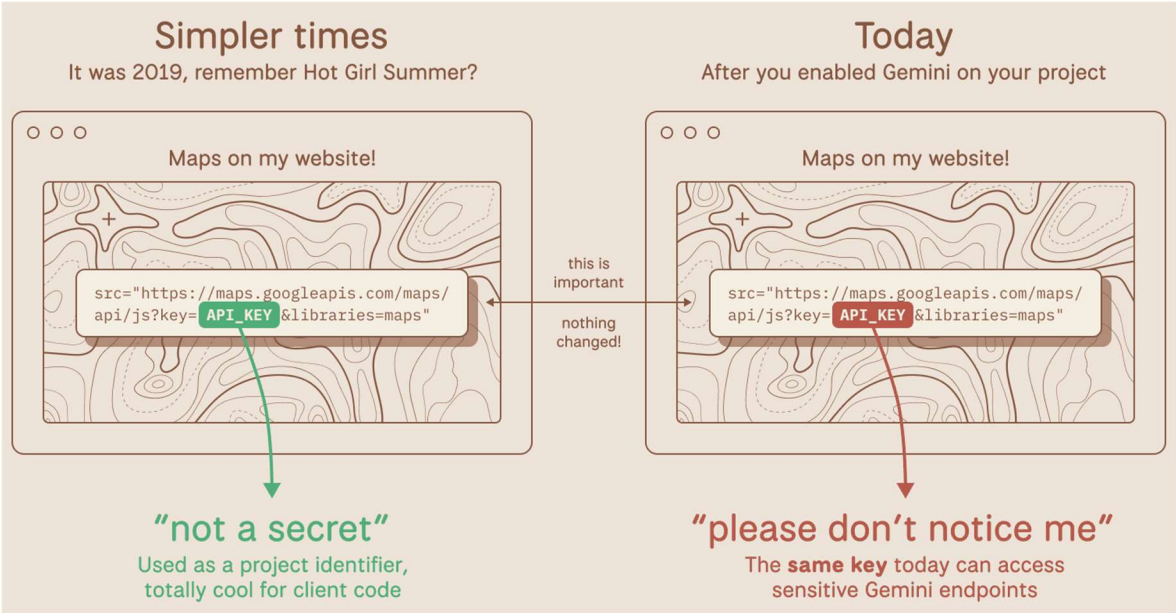


Figure 1 API Keys Today - Image: Trufflesecurity

Then came Gemini

When Google introduced its AI assistant, the same API keys suddenly gained a new, dangerous capability: they could authenticate to the Gemini API. Keys that had been sitting exposed in JavaScript for years, some since at least February 2023, now acted as gateways to private AI data and billable compute.

The Discovery

Researchers scanned the November 2025 Common Crawl dataset, a snapshot of popular websites, and found:

- More than 2,800 live Google API keys publicly exposed in website code.
- Keys belonging to major financial institutions, security firms, and recruiting agencies.
- At least one key embedded in a Google product's public-facing website, deployed since early 2023.
- The key successfully called Gemini's API endpoint to list available models, proving it worked.

The Risk

Attackers who find these exposed keys can:

- Access private data available through the Gemini API service.
- Make API calls on the victim's account, with the victim paying the bill.
- Depending on the model and context window, max out API calls and generate thousands of dollars in daily charges on a single account.

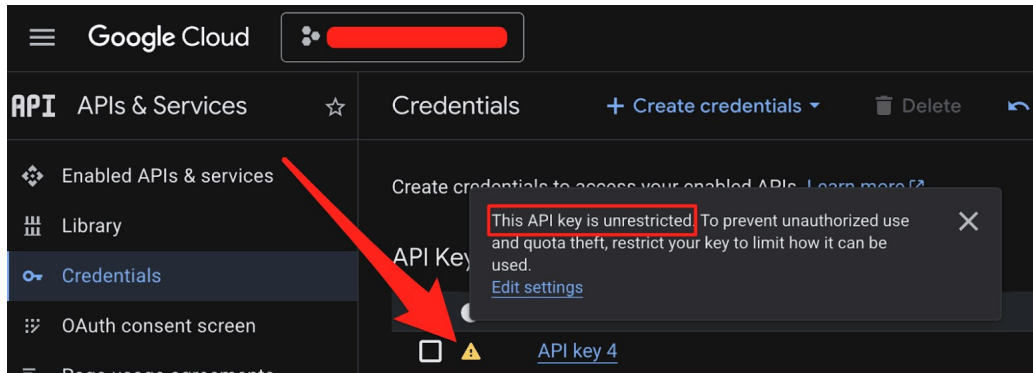
Timeline

- November 21, 2025: Researchers reported the issue to Google.
- January 13, 2026: After extended discussion, Google classified the flaw as "single-service privilege escalation."
- February 2026: Google announced mitigations and worked with researchers to address the issue.

Mitigation

If you or your organization have ever used Google Cloud API keys in client-side code, take immediate action:

- Check every GCP project for the Generative Language API. GCP console, navigate to APIs & Services > Enabled APIs & Services, and look for the "Generative Language API." If it's not enabled, you're not affected by this specific issue.
- Check if Gemini (Generative Language API) is enabled on your Google Cloud projects.
- Audit all API keys in your environment to determine if any are publicly exposed. Navigate to APIs & Services > Credentials. Check each API key's configuration. You're looking for two types of keys:
 - Keys that have a warning icon, meaning they are set to unrestricted
 - Keys that explicitly list the Generative Language API in their allowed services



- Rotate exposed keys immediately.
- Review your website's source code and remove any hardcoded API keys.
- Use proper authentication methods for Gemini, such as OAuth or service accounts with restricted permissions.

API keys that were once harmless identifiers can gain dangerous new capabilities when platforms evolve. The keys exposed in your website's JavaScript from 2023 may now be the keys to your AI data and your wallet. As more organizations bolt AI capabilities onto existing platforms, the attack surface for legacy credentials expands in ways nobody anticipated.

Ready to see how AICenturion can secure you against AI risks?

Request a demo today: hello@cytex.io

Connect with our social media channels

