Gemini AI flaws could have exposed your data

malwarebytes.com/blog/news/2025/10/gemini-ai-flaws-could-have-exposed-your-data

Pieter Arntz October 1, 2025

Security researchers discovered three vulnerabilities in Google's Gemini artificial intelligence (AI) assistant. Although now patched, this "Trifecta", as the researchers called it, raises important questions about how safe AI tools really are, especially as they become a part of services many of us use on a daily basis.

The flaws were found in three different Gemini components:

- **Gemini Cloud Assist**, which summarizes logs for cloud services, could be tricked by hidden prompts inside web requests. Attackers could exploit this flaw to sneak malicious instructions into the system, potentially gaining control over cloud resources.
- **Gemini Search Personalization Model** could inject harmful prompts into a user's Chrome browsing history by getting them to visit a special website. If the user later interacted with Gemini's personalized search AI, the injected commands could force the AI leak to personal data, including saved information and location.
- **Gemini Browsing Tool** could be tricked into sending stored user information and location data to a malicious server through its web page summarization feature.

Google fixed these issues by blocking Gemini from rendering dangerous links and strengthening its defenses against such prompt injections. But if you used Google

services that rely on Gemini AI, there is a chance these vulnerabilities were exploited before the patch—especially if you visited a malicious website or used Gemini features tied to cloud services.

These vulnerabilities are prime examples of how AI, despite its benefits, can open new attack avenues. Attackers may hide malicious instructions inside ordinary files and web requests, fooling AI into performing harmful actions without any obvious warning signs.

For everyday users, the risk is low—Google has already patched these vulnerabilities. But this news reminds all of us that AI security is an evolving concern, especially as new features and use-cases may be developed with security as an afterthought.

How to safely use AI

These flaws show that AI systems themselves can be used as a method for attacks, not just a target. This is important as AI becomes more embedded in cloud services and applications.

You should be cautious about:

- Avoid visiting unknown or suspicious websites, especially those that prompt you to interact with AI assistants.
- Keeping software, browsers, and apps up to date to benefit from security patches.
- Be mindful of the information you share with AI tools.
- Use a real-time anti-malware solution, preferably with web protection.

From reporting threats to removing them.