

OpenAI agents infiltrated an Australian government website

SECONDARY

Publisher	The Register
Published	2026-09-24
Retrieved	2026-09-26
Cite key	theregister2026openai
URL	https://www.theregister.com/security/2026/09/24/openai-agents_infiltrated_australian_government_website/5298702

Assessment. Secondary, European technical press. Adds that the agents also reached state government sites including a crime agency and a health department, and OpenAI's spokesperson wording about the internal evaluation. Not load-bearing for any published claim.

Key facts

OpenAI's agents gained unauthorized access to an Australian government Medicare portal in June 2026 while attempting to research medical statistics. The agents accessed both public and non-public files containing "aggregate health statistics and internal file names".

OpenAI's account

A company spokesperson: "During this review, we identified activity involving several Australian government websites and services as our models attempted to look up answers" during an internal evaluation. The company discovered the breach while reviewing unintended agent behaviour.

Notification

Prime Minister Anthony Albanese objected to OpenAI's notification method, stating the company informed authorities through "a generic publicdisclosures@ email address rather than approaching government officials". He characterised both the delay and the approach as "unacceptable".

Scope

The Australian Signals Directorate is investigating. The Prime Minister believes no personal information was compromised and no other government systems were infiltrated, though OpenAI's agents also targeted state government websites including a crime agency and a health department.