

GOOGLE REQUIRES AFFECTED AGENT STUDIO APPS TO BE REGENERATED AND REDEPLOYED

OPERATIONAL SIGNAL

DOMAIN: GOV —Governance & Security | CONFIDENCE LEVEL: Medium-High

INSTITUTIONAL DIMENSIONS: Authority | Attribution | Visibility | Escalation | Continuity

Signal ID	Platform	Source	Audience	Status	Date
SIG-GOV-004	Google Agent Studio	Link	Security IT Risk Ops	Pilot	2026-07-23

CAPABILITY SHIFT

Google has fixed a Server-Side Request Forgery vulnerability in backend code generated for Agent Studio web apps. The /api-proxy endpoint could send requests beyond approved destinations. Google now applies stricter domain validation. Organisations that downloaded, generated or deployed this code before 1 July 2026 must regenerate the app and deploy the new version.

ORGANISATIONAL CONSEQUENCE

The fix is contained in newly generated code, not previously deployed copies. Organisations must therefore identify affected apps, regenerate them, test the updated version and redeploy it. Teams may struggle to find every deployment where records are incomplete or the original developer has moved on.

WHAT TO WATCH

- Apps still running pre-1 July generated code
- Unknown app generation or deployment dates
- Regenerated apps awaiting testing or redeployment
- Further fixes requiring customer-side action

WHY THIS MATTERS NOW

Google disclosed the issue on 20 July. As of 23 July, earlier code may still be deployed. Remediation requires customer action; deployed copies will not update automatically.

WHAT TO REVIEW

- Which Agent Studio apps were generated, downloaded or deployed before 1 July
- Whether affected apps have been regenerated and redeployed
- Whether earlier /api-proxy endpoints were externally reachable
- Whether records identify all affected apps
- Whether updated apps require security or regression testing
- Whether security reviews cover platform-generated code

GOVERNANCE CONTEXT

This illustrates an ownership issue in generated software: a vendor may fix the generator while customers remain responsible for finding and replacing previously deployed outputs.

Scope Boundary: This artefact translates observed platform capability changes into operational considerations. It does not constitute policy, legal advice, or enforcement guidance.