Human approval design for security agents

APPROVAL RECORD AP-0412
Proposed by: remediation agent, run 7f3a, 19 Nov 2026 09:14
Finding: CVE-2026-75604, Next.js incremental-cache path traversal, CVSS 9.0 (GitHub CNA)
Asset: orders-web, Windows host, internet-facing
Change: package.json next 15.5.9 -> 15.5.24; lockfile regenerated; rebuild and redeploy
Why: affected range is >= 13.4.0 and < 15.5.24 on a Windows filesystem. The vendor states no workaround exists for affected Windows-hosted applications.
Checks already run: build passed; 212 of 212 tests passed; rescan of the staging build shows next 15.5.24
Not determined by the agent: whether the app uses the App Router with Cache Components (the advisory covers Pages Router, or App Router without Cache Components); the router setting is not in the files the agent read
Undo: redeploy build 0411; about 10 minutes
Decision options: approve / edit / reject with reason
Approver: ____ Time seen: ____ Decision: ____ Reason if edited or rejected: ____

Agentic AI in Cybersecurity, Human approval design for security agents, edition 19 Nov 2026, https://agenticaiincybersecurity.com/guides/human-approval-design/. License CC BY 4.0.