What is GitHub App token abuse?

A GitHub App installation can mint short-lived access tokens scoped to a repository's granted permissions. An attacker who compromises the App's private key or a runner that carries the installation mints fresh tokens with scopes like contents:write and pull_requests:write, then reads private repositories, pushes code, or opens malicious pull requests. Defend by protecting the App key, minimising installation scopes, and monitoring token minting.

HOW IT WORKS

01 How it works and example

The attacker obtains the App's private key or lands on a CI runner that already holds the installation, then mints fresh installation tokens with write scopes. With contents:write and pull_requests:write they list internal repositories, read source for infrastructure details, push code, and open pull requests to trigger pipelines, as seen in a 2026 supply-chain intrusion.

SOURCES

[1] MITRE ATT&CK: Credential Access (TA0006)

[2] HuggingFace, Agent intrusion technical timeline

[3] MITRE ATT&CK: Steal Application Access Token (T1528)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/github-app-token-abuse

Open online