Astrix

Insecure third-party connections to your GitHub may trigger a supply chain attack

Do you really know how many third-party applications have access to your GitHub repository?

IT teams, DevOps, and developers are increasingly authorizing new third-party applications to access the organization's GitHub repositories in a bid to boost productivity. However, many of these are **shadow integrations** (connected via API keys, service accounts, webhooks, OAuth tokens, or even SSH keys) that are not vetted by security teams. They are also often over-privileged or were connected by users who have since left the company.

These unmonitored connections to your GitHub (of which there could be thousands) create a new ecosystem of supply chain dependencies that expand your attack surface and expose your organization to supply chain attacks, compliance violations, and unauthorized access.

Organizations should protect their API keys as vigorously as they protect their passwords. Leaking an API key can be more consequential than leaking a username and password login since logins are often protected by two-factor authentication nowadays, whereas API keys are not.

The threat is real

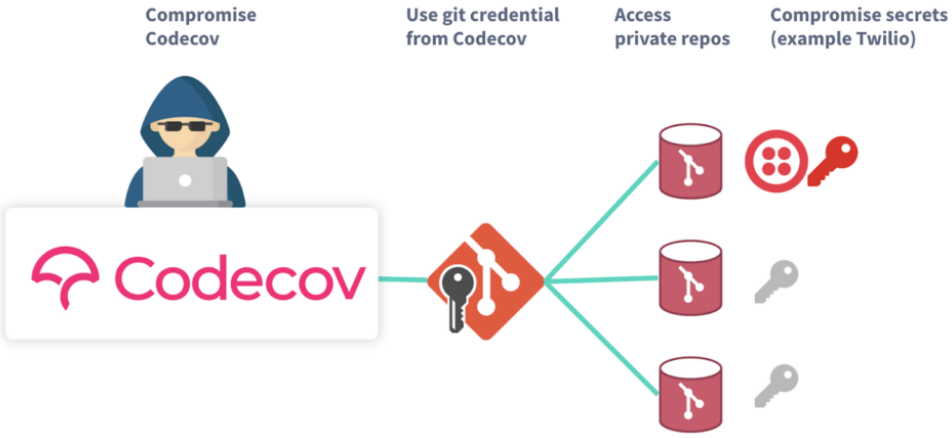
GitHub attacks triggered by third-party integrations

Recent high-profile attacks targeting Github reveal a new generation of supply chain attacks, in which attackers take advantage of access granted to third-party cloud services as a backdoor into GitHub repositories.

- **September 16, 2022:** Following a phishing campaign targeting GitHub users, which impacted many victim organizations, GitHub has warned their customers about one of the tactics used by the threat actor - “If the threat actor successfully steals GitHub user account credentials, they may quickly create GitHub personal access tokens (PATs), authorize OAuth applications, or add SSH keys to the account in order to preserve access in the event that the user changes their password.”

- **April 12, 2022:** Attackers used stolen OAuth app tokens issued to Heroku and Travis-CI to breach dozens of GitHub customer accounts with authorized Heroku or Travis CI OAuth app integrations.

- **April 1, 2021:** In the Codecov breach, attackers compromised the Codecov cloud service and stole OAuth tokens that provided them with direct access to the GitHub repositories of 17,000 CodeCov customers. (see an example of this attack against Twilio company in caption A below).



Codecov and Twilio Attack flow (Source)

- **June 16, 2022:** GitHub sent a message to its customers disclosing a bug in GitHub Apps that existed for a 5-day timeframe between February 25 and March 2, 2022 – and which could have been abused to grant excessive permissions to malicious third-party applications

GitHub integration risks found in real organizations' engineering environments

From our research among organizations of over 1,000 employees, we discovered GitHub environments have:

- Thousands of connections to third-party applications and cloud services
- The majority of connections are shadow connections, connected with API keys, Webhooks and even SSH keys (in comparison to only dozens of integrations to GitHub apps)
- On average, 4-5 new integrations are added, on a weekly basis

As a result, there is simply too much data for security teams to review to ensure that all GitHub integrations are secure. And while the GitHub admin console tracks access credentials and app integrations, it doesn't identify untrusted or insecure configurations, apps, or integrations.

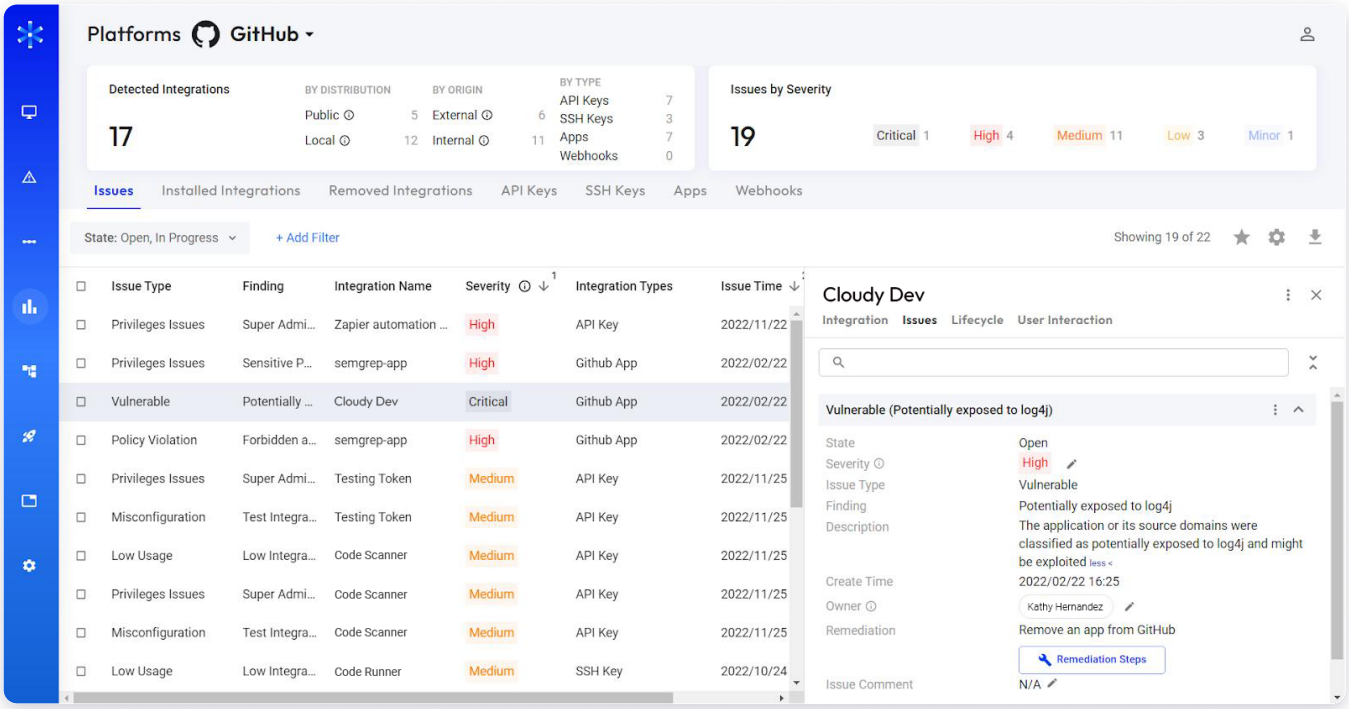
Using the Astrix Security platform, our customers discovered that their GitHub environment is far more exposed to third-party cloud services than they thought, with the average number of connections 10x more than the estimated number. The troubling findings include:

- **Redundant access:** 40% of the SSH and API keys configured to access GitHub repos were no longer in active use, or connected by employees who had since left the company.
- **Over-privileged access:** Connections with common cloud services (Heroku, Codecov, Travis CI, etc) were configured with admin permissions.
- **Dangerous practices:** Unencrypted webhooks exposed sensitive data to the network by transmitting it to cloud services.
- **Untrusted vendors:** Connections with third-party apps and services of low-reputation publishers.

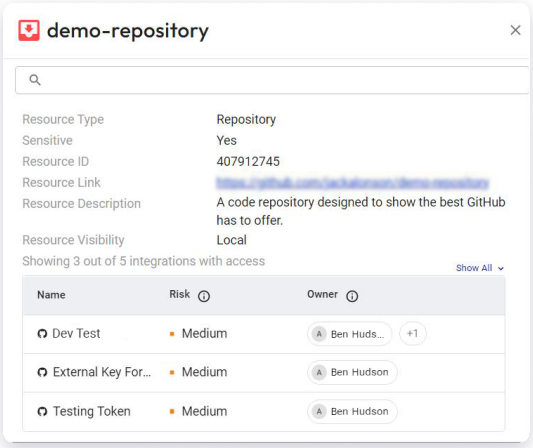
How to ensure your GitHub is securely connected to cloud-services with Astrix

Astrix Security Platform allows GitHub users to be productive while also ensuring robust security by delivering:

- **Holistic visibility:** Astrix provides a consolidated, comprehensive view of all third-party integrations with your GitHub repositories. You get complete visibility into which external services can access your GitHub resources, as well as the level of access and permissions granted to each one.

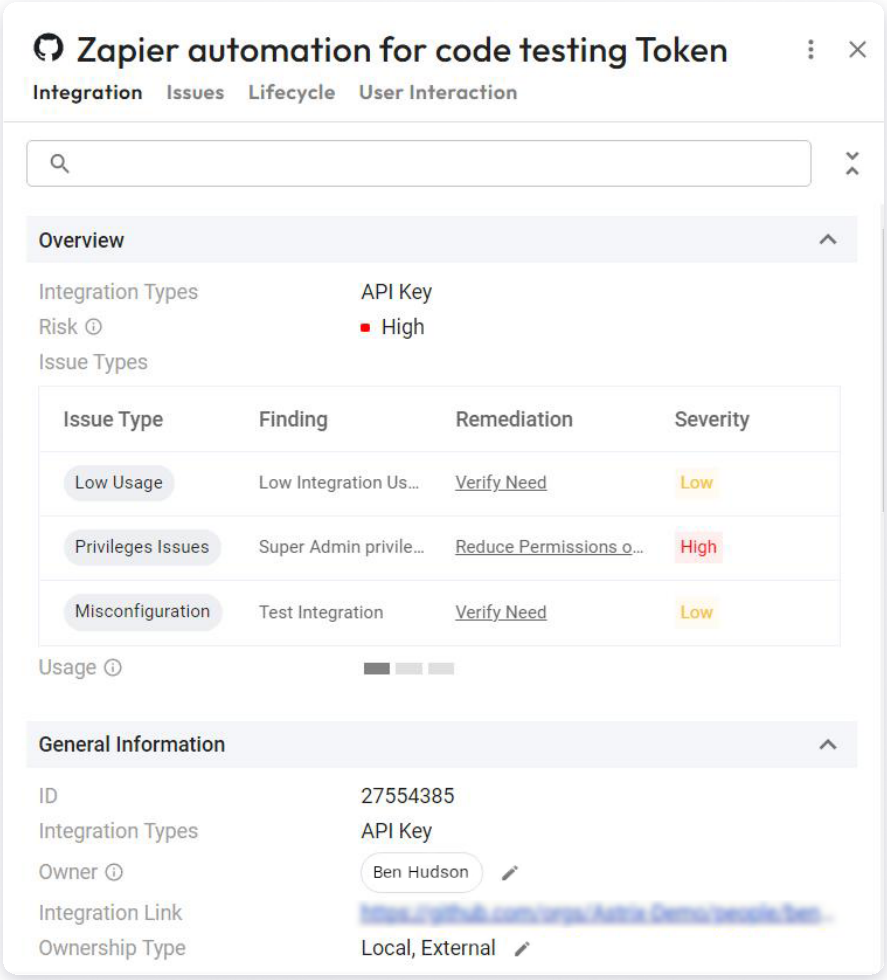


Here, the Astrix Security Platform pinpoints the most critical integration issues. One of the issues highlighted here is a high-risk integration with a cloud service named “Cloudy Dev”, which can be exploited by a threat actor using the Log4J vulnerability.



Here, the Astrix Security Platform, allows you to deep dive into specific Git repositories that the organization considers as “sensitive,” see all the integrations that have access to these repositories and assess the potential risk accordingly.

- **Threat detection:** Astrix automatically Identifies malicious third-party integrations, anomalous behavior (like suspicious source IPs), overly permissive integrations, redundant applications and insecure tokens. That means you know where GitHub risks lie and how they can be exploited.



Here, the Astrix Security Platform enables you to deep-dive into a specific connection (integration). In this example, we see a connection created by a developer that has generated an API key granting access to a third-party cloud service called “Zapier Automation for Code Testing”. The platform alerts the security team that this is a high-risk connection since it has super-admin permissions, hasn’t been in use lately, and is misconfigured.

- **Rapid remediation:** By automating remediation workflows, integrating with your daily IT service management tools, and enabling end-users to resolve security issues in the process, Astrix can automatically remediate your GitHub security risks. This helps take the burden off of your IT team. Security admins Receive highly digested security alerts, including user feedback, threat context, severity level, and suggested remediation steps.

Learn more

Stay up-to-date with the latest in third-party integration threat prevention by downloading our free eBook, "The Ultimate Guide to Securing App-to-App Integrations."

Or, contact us to discuss your business's GitHub security risks and how Astrix can solve them.