



Flash Report

GitHub Repositories Targeted in Malicious Cyber Activity

F-2025-03-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Consent Phishing, OAuth Abuse, Supply Chain Compromise

March 19, 2025

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on March 19, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | GitHub Repositories Targeted in Malicious Cyber Activity

| Key Findings

- Since approximately March 14, 2025, GitHub repositories have been targeted in two likely separate malicious cyber campaigns, resulting in the likely compromise of user credentials, accounts, and sensitive information associated with continuous integration (CI) and continuous delivery (CD) tools.
- At least 12,000 separate repositories have reportedly been targeted in a phishing campaign that leverages open authorization (OAuth) abuse to deceive users into granting attackers access to accounts and credentials.
- The seemingly separate targeting of GitHub Actions via a supply chain compromise tracked by the National Institute of Standards and Technology (NIST) as CVE-2025-30066 was also first reported on March 14, 2025.
- Subsequent research suggests that this initial incident may have facilitated the more recent targeting of the “tj-actions/changed-files” Action. As of the writing of this report the full extent of this activity is unclear, but there is a very likely chance that associated GitHub Actions remain compromised.

Details

Since approximately March 14, 2025, GitHub repositories have been targeted in two likely separate malicious cyber campaigns, resulting in the likely compromise of user credentials, accounts, and sensitive information associated with CI and CD tools.

At least 12,000 separate repositories have reportedly been targeted in a phishing campaign that leverages OAuth abuse to deceive users into granting attackers access to accounts and credentials.¹

- OAuth is an authorization framework that provides legitimate access to resources hosted by other web applications. The associated permissions are being increasingly exploited by malicious actors as a means to access user accounts without possession of login credentials, while also circumventing multi-factor authentication (MFA) protocols.

According to social media posts by numerous GitHub users, attackers send security alert emails that purport to be from the GitHub security team and advise recipients that their accounts have been subjected to unusual access attempts. Upon following the notification's instructions, users are directed to "gitsecurityapp"—an OAuth application that proceeds to request the following extensive user permissions:

- repo: Grants comprehensive access to public and private repositories
- delete repo: Grants permission to delete repositories
- read:org: Grants read-only access to memberships and organizations
- write/discussion: Grants read and write permissions for discussions
- gist: Grants permission to create, modify, and delete gists
- workflows, workflow, write:workflow, read:workflow, update:workflow: Grants general, read, and edit permissions to workflow files
- user: Grants permission to read and write profile information

¹ [hXXps://x\[.\]com/luc4m/status/1901271981615448094](https://x.com/luc4m/status/1901271981615448094)

Security Alert: Unusual Access Attempt

We have detected a login attempt on your GitHub account that appears to be from a new location or device.

Login Information

- **Location:** Reykjavik, Iceland
- **IP Address:** 53.253.117.8
- **Device:** Unrecognized

If you recognize this activity, no further action is required. However, if this was not you, we strongly recommend securing your account immediately.

Steps to Secure Your Account

1. **Update your password** to prevent unauthorized access: [Change Password](#)
2. **Review and manage active sessions:** [Check Recent Activity](#)
3. **Enable Two-Factor Authentication (2FA)** for additional protection: [Set Up 2FA](#)

Contact Support

If you need assistance or suspect a security breach, visit: [GitHub Security Support](#)

Thank you for keeping your account secure.

GitHub Security Team

Fraudulent GitHub security alert sent to users

Source: X (formerly, Twitter)

Of these permissions, repo and workflow access likely pose the greatest threat to the majority of developers, as they potentially grant the attacker access to sensitive source code or unencrypted API keys. The extent of access afforded is heavily dependent on user security practices. Other permissions, such as gist and user, could potentially allow the attacker to obtain personally identifiable information (PII).

The login information provided by the malicious communications lists the device that allegedly attempted an unauthorized login as “unspecified” and located in Reykjavik, Iceland. However, users have reported two separate internet protocol (IP) addresses being utilized: 53.253.117[.]8 and 188.253.117[.]8.

- Upon inspection, neither of these IP addresses appear to be associated with Reykjavik, Iceland. Rather, they emanate from Germany and Taiwan, respectively.

The seemingly separate targeting of GitHub Actions via a supply chain compromise tracked by NIST as CVE-2025-30066 was also first reported on March 14, 2025.²³ The incident reportedly began with the compromise of GitHub Action “reviewdog/action-setup@v1”, a set-up tool for code review tool ReviewDog.⁴

Subsequent research suggests that this initial compromise may have facilitated a more recent breach via the targeting of the “tj-actions/changed-files” Action, which uses the reviewdog/action-setup@v1 GitHub Action. This incident reportedly led to the leak of CI and CD sensitive information taken from build logs to thousands of repositories, which could have enabled their theft.

The full extent of compromise is currently unclear, but there is a very likely chance that the following GitHub Actions remain compromised:

- reviewdog/action-shellcheck
- reviewdog/action-composite-template
- reviewdog/action-staticcheck
- reviewdog/action-ast-grep
- reviewdog/action-tpos
- reviewdog/action-setup

As of the writing of this report, any targeting patterns, additional indicators of compromise (IoCs), and tactics, techniques, and procedures (TTPs) that may allude to a threat actor being this malicious activity are unclear or unavailable. However, GitHub’s widespread use amongst corporate entities, and its critical function within many software supply chains, almost certainly renders associated repositories, actions, and workflows, appealing targets to state-associated cyber entities seeking to further cyber espionage initiatives, as well as malicious actors seeking to disrupt associated software supply chains.

² [hXXps://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised](https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised)

³ [hXXps://nvd.nist.gov/vuln/detail/CVE-2025-30066](https://nvd.nist.gov/vuln/detail/CVE-2025-30066)

⁴ [hXXps://www.wiz.io/blog/new-github-action-supply-chain-attack-reviewdog-action-setup](https://www.wiz.io/blog/new-github-action-supply-chain-attack-reviewdog-action-setup)

Recommendations

- GitHub users should not use the tj-actions/changed-files Action. Remove references from all branches of repositories and Action lists.
- Follow the most up-to-date threat research to understand how this compromise may affect personal or organizational repositories.
 - [hXXps://github\[.\]com/advisories/GHSA-mrrh-fwg8-r2c3](https://github.com/advisories/GHSA-mrrh-fwg8-r2c3)
 - [hXXps://www.cisa\[.\]gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-github-action-cve-2025-30066](https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-github-action-cve-2025-30066)
- Organizations should ensure that employees receive training covering contemporary social engineering threats and TTPs, including consent phishing.
- Ensure that employees are aware of the threats posed by OAuth abuse and the granting of permissions to malicious actors.
- Scrutinize all digital communications, even if appearing to originate internally. Look for incorrect or unusual grammar and language, spelling mistakes, mismatched URLs, and illegitimate sender addresses.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate critical network areas.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%