EnCyb

Severity: High

Advisory Type: Security

AWS CodeBuild Vulnerability

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

A security misconfiguration affecting AWS CodeBuild has been identified that may expose GitHub repositories and sensitive CI/CD secrets, creating a software supply chain attack risk. When CodeBuild projects are configured to automatically build untrusted pull requests or external forks without proper isolation, attackers can abuse the build environment to exfiltrate credentials or inject malicious code into build artifacts.

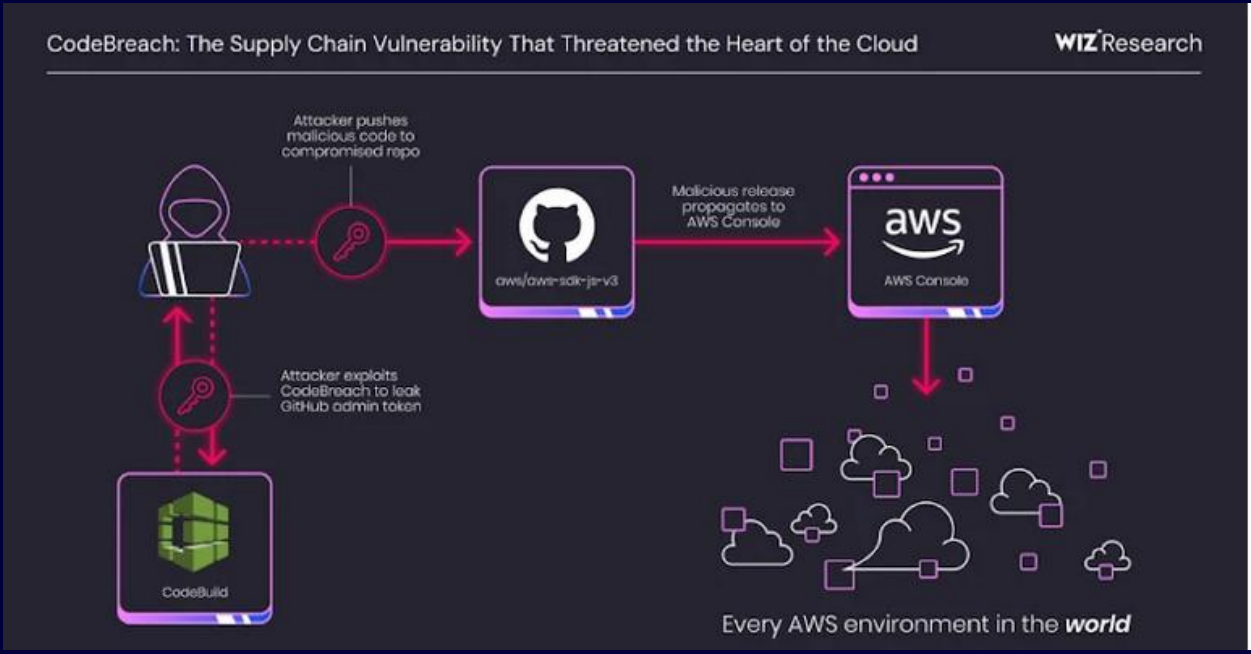
This issue does not stem from a software vulnerability but from insecure CI/CD trust boundaries and IAM misconfigurations, which can allow attackers to poison software builds and compromise downstream consumers.

- Active Region: Global
- Affected Sector: Software Development, Cloud Services
- Affected Product: AWS CodeBuild (GitHub-integrated CI/CD pipelines)
- Severity: High
- Published Date: January 15, 2026

TECHNICAL DETAILS

- **Attack Vector:** Remote exploitation via malicious pull requests or forked repositories submitted to GitHub projects integrated with AWS CodeBuild. No AWS authentication is required; attackers only need the ability to trigger an automated build.
- **Affected Components / Platforms:** AWS CodeBuild projects integrated with GitHub or GitHub Enterprise across all AWS regions, especially pipelines configured to automatically build external pull requests.
- **Exploitation Impact:** Successful exploitation can result in credential exfiltration (GitHub tokens, AWS keys), unauthorized access to private repositories, injection of malicious code into build artifacts, and broader software supply chain compromise.

ATTACK WORKFLOW



Software supply chain attack (CodeBreach) where an attacker injects malicious code into a compromised GitHub repository. This malicious code is built automatically by AWS CodeBuild, which leaks a GitHub admin token. The attacker then publishes a malicious release that propagates through the AWS Console, potentially impacting any AWS environment worldwide that relies on the affected SDK or package.

IMPACT

- **Credential Exposure**: GitHub tokens, AWS credentials, and third-party API keys may be leaked.
- **Supply Chain Compromise**: Malicious code can be introduced into software artifacts, libraries, or container images.
- **Lateral Movement**: Compromised credentials can be reused to access additional repositories or cloud services.
- **Trust & Compliance Risk:** Undermines secure SDLC practices and may violate SOC 2, ISO 27001, or regulatory controls.

RECOMMENDATIONS

- Disable automatic builds for untrusted pull requests.
- Apply least-privilege IAM policies to CodeBuild service roles.
- Separate pipelines for trusted vs untrusted contributors.
- Enable centralized logging (CloudTrail, CloudWatch, GitHub Audit Logs).
- Require manual approval for external PR builds.

REFERENCE

- https://thehackernews.com/2026/01/aws-codebuild-misconfiguration-exposed.html
- https://www.wiz.io/blog/wiz-research-codebreach-vulnerability-aws-codebuild

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com