مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Command Injection Vulnerability in GitHub Action Workflow

Tracking #:432317548

Date:30-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical command injection vulnerability in a popular GitHub Action workflow. This flaw could allow attackers to execute arbitrary commands within CI/CD workflows, posing a severe threat to the integrity of automation pipelines.

TECHNICAL DETAILS:

A critical command injection vulnerability exists in the *tj-actions/branch-names* GitHub Action, where unsafe use of *eval* allowed attackers to execute arbitrary shell commands by crafting malicious branch or tag names. This vulnerability could compromise CI/CD workflows, leading to unauthorized access, data exfiltration, or code tampering.

Vulnerability Details:

- **Vulnerability ID:** CVE-2025-54416
- **CVSS Score:** 9.1 (Critical)
- **Affected Component**: *tj-actions/branch-names* GitHub Action
- **Affected Versions**: All versions prior to v9.0.0
- **Fixed Version**: v9.0.0 and later
- **Exploit Vector**: Malicious branch or tag names triggering command execution via CI workflows

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-54416