مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in Google Gemini CLI

Tracking #:432319209

Date:29-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has disclosed a critical security vulnerability, CVE-2026-12537, affecting the Google Gemini CLI and the run-gemini-cli GitHub Action.

TECHNICAL DETAILS:

Google has disclosed a critical security vulnerability, CVE-2026-12537, affecting the Google Gemini CLI and the run-gemini-cli GitHub Action. The vulnerability is rated CVSS v4 10.0 (Critical), representing the highest possible severity.

The flaw allows unauthenticated remote code execution (RCE) in automated Continuous Integration/Continuous Deployment (CI/CD) environments through improper handling of malicious environment files. An attacker can exploit the vulnerability by submitting a specially crafted pull request containing a malicious environment file, causing arbitrary operating system commands to execute during automated workflow runs.

Successful exploitation could lead to complete compromise of CI/CD infrastructure, including theft of secrets, modification of source code, deployment pipeline compromise, and lateral movement into connected environments.

Although no active exploitation or public proof-of-concept (PoC) has been reported, organizations using affected versions should treat this as an emergency patching priority.

Vulnerability Details:

- CVE ID: CVE-2026-12537
- Vulnerability Type: OS Command Injection leading to Remote Code Execution (RCE)
- Severity: Critical
- CVSS v4 Score: 10.0 (Maximum Severity)
- Affected Products:
  - Google Gemini CLI versions prior to 0.39.1
  - run-gemini-cli GitHub Action versions prior to 0.1.22
- Fixed Versions:
  - Google Gemini CLI 0.39.1 or later (including 0.40.0-preview.3)
  - run-gemini-cli GitHub Action 0.1.22 or later

RECOMMENDATIONS:

Immediate Actions:

- Immediately upgrade to the patched versions, review GitHub Actions workflows, enable explicit workspace trust, and harden CI/CD pipelines against untrusted inputs.

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://github.com/google-github-actions/run-gemini-cli/security/advisories/GHSA-wpqr-6v78-jr5g