مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Spring Cloud Config

Tracking #:432318914

Date:07-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity vulnerabilities have been disclosed in the Spring Cloud Config project, a widely used component for centralized configuration management in distributed systems.

TECHNICAL DETAILS:

Multiple high-severity vulnerabilities have been disclosed in the Spring Cloud Config project, a widely used component for centralized configuration management in distributed systems. The most critical issue (CVE-2026-40982, CVSS 9.1) enables directory traversal, allowing unauthenticated attackers to read arbitrary files from the server. Additional flaws impact Google Cloud Platform (GCP) secret isolation, Git repository integrity, and logging mechanisms, potentially leading to credential exposure and cross-environment data leakage.

Vulnerability Details:

1. CVE-2026-40982 – Directory Traversal (Critical | CVSS 9.1)
   - Component Affected: spring-cloud-config-server
   - Impact: Arbitrary file read on host filesystem
   - Attack Vector: Crafted URL request exploiting file path traversal

Key Risk:
   - Exposure of system files (e.g., /etc/passwd, configuration files, application secrets)
   - Potential retrieval of cloud credentials stored locally
   - No authentication required in some configurations

2. CVE-2026-40981 – GCP Secret Exposure (High | CVSS 7.5)
   - Component Affected: Google Secrets Manager backend integration
   - Impact: Cross-project secret leakage in GCP environments

Key Risk:
   - Breaks isolation between GCP projects
   - Allows retrieval of secrets from unintended projects
   - Exposure of API keys, service accounts, and environment-specific credentials

3. CVE-2026-41002 – Git TOCTOU Attack (High | CVSS 7.2)
   - Component Affected: Git repository backend in Config Server
   - Impact: Race condition between file validation and usage
   - Attack Type: Time-of-Check-Time-of-Use (TOCTOU)

Key Risk:
   - Manipulation of repository directory during cloning process
   - Unauthorized file access or modification
   - Potential injection of malicious configuration artifacts

4. CVE-2026-41004 – Sensitive Data Leakage via Logs (Medium | CVSS 4.4)
   - Component Affected: Logging subsystem (trace logging enabled)
   - Impact: Exposure of secrets in plaintext logs

Key Risk:
   - Credentials and configuration values written to logs
   - Unauthorized access via log aggregation systems (e.g., SIEM, ELK)

- Persistent exposure if logs are not rotated or sanitized

Affected Versions:

- Spring Cloud Config:
  - 3.1.x
  - 4.1.x
  - 4.2.x
  - 4.3.x
  - 5.0.x
  - Older unsupported versions (higher risk due to lack of patches)

Fixed Versions:

- 4.3.3
- 5.0.3

RECOMMENDATIONS:

Immediate Patch Deployment

- Upgrade all Spring Cloud Config deployments to fixed version.

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://spring.io/security