مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Spring Boot

Tracking #:432318843

Date:27-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that multiple high-impact vulnerabilities have been disclosed in Spring Boot, a widely used Java framework.

TECHNICAL DETAILS:

Multiple high-impact vulnerabilities have been disclosed in Spring Boot, a widely used Java framework underpinning millions of enterprise applications. The most critical flaw (CVSS 9.1) can completely bypass application security controls under specific configurations, exposing all endpoints to unauthorized access.

Vulnerability Details:

1. Authentication Bypass via Default Security Misconfiguration
   - **CVE ID: CVE-2026-40976**
   - Severity: Critical (CVSS 9.1)
   - Component: Default Web Security Configuration (via Spring Security)

Key Issue:
   - A flaw in the default security filter chain may result in complete security bypass, leaving all endpoints unprotected.

Conditions for Exploitation:
   - Application is servlet-based.
   - Relies solely on default security configuration (no custom security rules).
   - Includes spring-boot-actuator-autoconfigure.
   - Does not include spring-boot-health dependency.

2. Timing Attack in DevTools Leading to Secret Disclosure
   - **CVE ID: CVE-2026-40972**
   - Severity: High (CVSS 7.5)
   - Component: Spring Boot DevTools

Key Issue:
   - A timing side-channel vulnerability allows attackers to infer secrets by measuring response times.

Attack Vector:
   - Attacker must be on the same network.
   - Exploits non-constant-time comparison of secrets.

3. Insecure Temporary Directory Handling
   - **CVE ID: CVE-2026-40973**
   - Severity: High (CVSS 7.0)
   - Component: ApplicationTemp Directory Handling

Key Issue:
   - Predictable or controllable temporary directory usage.

Attack Vector:
   - Requires local access to the host system.
   - Execute arbitrary code using crafted gadget chains.
   - Privilege escalation within application context.

Affected Versions & Fix Availability

- 4.0.x → Fixed in 4.0.6 (OSS)
- 3.5.x → Fixed in 3.5.14 (OSS)
- 3.4.x → Fixed in 3.4.16 (Enterprise only)
- 3.3.x → Fixed in 3.3.19 (Enterprise only)
- 2.7.x → Fixed in 2.7.33 (Enterprise only)

RECOMMENDATIONS:

- Upgrade Immediately: Upgrade Spring Boot to fixed version at the earliest.

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/cve-2026-40976
- https://spring.io/security/cve-2026-40972
- https://spring.io/security/cve-2026-40973