مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in Fastjson

Tracking #:432319342

Date:27-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability, CVE-2026-16723, has been disclosed in Alibaba Fastjson.

TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability, CVE-2026-16723, has been disclosed in Alibaba Fastjson 1.x, with a CVSS v3 score of 9.0 (Critical). Public technical details and proof-of-concept (PoC) exploit code are now available, significantly increasing the likelihood of exploitation.
Security researchers and threat intelligence providers have reported active exploitation targeting organizations across multiple sectors, including financial services, healthcare, retail, technology, and other enterprise environments. The vulnerability enables unauthenticated remote code execution under Fastjson's default configuration, eliminating several previously assumed security protections.

Vulnerability Details:

- **CVE ID:** CVE-2026-16723
- **Vulnerability Type:** Remote Code Execution (RCE)
- **Severity:** Critical
- **CVSS v3 Score:** 9.0
- **Affected Product:** Alibaba Fastjson 1.x
- **Affected Versions:** Fastjson 1.2.68 through 1.2.83 (including the final 1.x release)
- **Attack Vector:** Network
- **Authentication Required:** No
- **User Interaction Required:** None
- **Privileges Required:** None
- **Exploitation Status:** Actively exploited in the wild
- **Public Proof-of-Concept (PoC):** Available
- **Root Cause:** Improper handling of polymorphic deserialization and internal type resolution using the @type field.
- **Default Configuration Impact:** Exploitable under Fastjson's default configuration; AutoType does not need to be enabled.
- **Third-Party Gadget Requirement:** No third-party gadget classes are required for successful exploitation.
- **Technical Mechanism:** Attackers can craft malicious JSON payloads containing a manipulated @type value to bypass Fastjson's type restrictions.
- **Exploitation Technique:** Abuses Fastjson's internal type-resolution logic and nested JAR URL handling in Spring Boot fat-JAR deployments to achieve code execution.
- **Affected Platforms:** Verified on Spring Boot 2.x, 3.x, and 4.x running JDK 8, 11, 17, and 21.

RECOMMENDATIONS:

Immediate Actions:

- Identify all applications using Fastjson 1.x.
- Enable SafeMode immediately.
- Migrate all applications from Fastjson 1.x to Fastjson 2.x after compatibility testing.
- Remove deprecated Fastjson 1.x dependencies from build pipelines.

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/alibaba/fastjson2/wiki/Security-Advisory%3A-Remote-Code-Execution-in-fastjson-1.2.68%E2%80%931.2.83