An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2607290226

NCSC Advisory

Critical vulnerability exists in Fastjson

CVE-2026-16723

29th, July 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-16723

Published: 2026-07-23

Vendor: Alibaba

Product: Fastjson

CVSS Score[1]: 9.0

Products Affected

Product	Version
Fastjson	1.2.68 <= 1.2.83

Impact

A remote code execution (RCE) vulnerability exists in fastjson 1.2.68 through 1.2.83. This vulnerability is exploitable under fastjson's stock default configuration — no AutoType enablement required, no classpath gadget required.

Common Weakness Enumeration (CWE)[2]:

- CWE-20: Improper input validation
- CWE-502: Deserialization of untrusted data

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Alibaba.

- https://nvd.nist.gov/vuln/detail/CVE-2026-16723
- https://www.cve.org/CVERecord?id=CVE-2026-16723
- https://github.com/alibaba/fastjson2/wiki/Security-Advisory:-Remote-Code-Execution-in-fastjson-1.2.68%E2%80%931.2.83