



CVE-2017-3203

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3203
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-11 17:29:00 UTC
Updated	2019-10-09 23:27:00 UTC
Description	The Java implementations of AMF3 deserializers in Pivotal/Spring Spring-flex derive class instances from java.io.Externaliz

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal	Spring-flex	All	All	All	All
Application	Pivotal	Spring-flex	All	All	All	All

References

Reference

- [code white | Blog: AMF – Another Malicious Format](#)
- [VU#307983 - Action Message Format \(AMF3\) Java implementations are vulnerable to insecure deserialization and XML external entities refer](#)
- [Flaws in Java AMF Libraries Allow Remote Code Execution | SecurityWeek.Com](#)
- [Pivotal Spring Flex CVE-2017-3203 Remote Code Execution Vulnerability](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)