



CVE-2017-12612

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

Summary

CVE	CVE-2017-12612
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-13 16:29:00 UTC
Updated	2017-09-26 16:25:00 UTC
Description	In Apache Spark 1.6.0 until 2.1.1, the launcher API performs unsafe deserialization of data received by its socket. This mak

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Spark	1.6.0	All	All	All
Application	Apache	Spark	1.6.1	All	All	All
Application	Apache	Spark	1.6.2	All	All	All
Application	Apache	Spark	1.6.3	All	All	All
Application	Apache	Spark	2.0.0	All	All	All
Application	Apache	Spark	2.0.1	All	All	All
Application	Apache	Spark	2.0.2	All	All	All
Application	Apache	Spark	2.1.0	All	All	All
Application	Apache	Spark	2.1.1	All	All	All
Application	Apache	Spark	1.6.0	All	All	All
Application	Apache	Spark	1.6.1	All	All	All
Application	Apache	Spark	1.6.2	All	All	All
Application	Apache	Spark	1.6.3	All	All	All
Application	Apache	Spark	2.0.0	All	All	All
Application	Apache	Spark	2.0.1	All	All	All
Application	Apache	Spark	2.0.2	All	All	All
Application	Apache	Spark	2.1.0	All	All	All

Application	Apache	Spark	2.1.1	All	All	All
References						
Reference		Source	Link	Tags		
Apache Spark CVE-2017-12612 Deserialization Remote Code Execution Vulnerability		BID	www.securityfocus.com	Third Party A		
CVE-2017-12612 Unsafe deserialization in Apache Spark launcher API		MISC	mail-archives.apache.org	Mailing List,		
CVE Program record		CVE.ORG	www.cve.org	canonical		
NVD vulnerability detail		NVD	nvd.nist.gov	canonical, a		
No vendor comments have been submitted for this CVE.						
Legacy QID Mappings						
981181 Java (maven) Security Update for org.apache.spark:spark-core_2.10 (GHSA-8rhc-48pp-52gr)						

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report