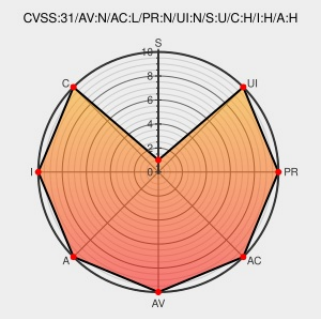
CVE-2019-17564

Published on: 04/01/2020 12:00:00 AM UTC

Last Modified on: 03/30/2021 11:15:00 PM UTC

CVE-2019-17564

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dubbo from Apache contain the following vulnerability:

Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. This issue affected Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.x versions.

CVE-2019-17564 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache** - **Apache Dubbo** version **2.7.0 to 2.7.4**

Affected Vendor/Software: **Apache** - **Apache Dubbo** version **2.6.0 to 2.6.7**

Affected Vendor/Software: **Apache** - **Apache Dubbo** version **all 2.5.x versions**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MISC lists.apache.org/thread.html/r13f7a58fa5d61d729e538a378687118e00c3e229903ba1e7b3a
No Description Provided	advisory.checkmarx.net text/html	MISC advisory.checkmarx.net/advisory/CX-2020-4275

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Basic code for creating the Alibaba FastJson + Spring gadget chain, as used to exploit Apache Dubbo in CVE-2019-17564…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Dubbo	All	All	All	All
Application	Apache	Dubbo	All	All	All	All
Application	Apache	Dubbo	All	All	All	All

cpe:2.3:a:apache:dubbo:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:dubbo:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:dubbo:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Apache - CVE-2019-17564: advisory.checkmarx.net/advisory/CX-20…	2021-03-31 00:43:39
@wallcorners	Giới thiệu về Apache Dubbo và phân tích CVE 2019-17564 codechay.com/tin-tuc-chung-…	2021-06-20 19:25:32
@DorTumarkin	Looks like the Apache Dubbo kicking party from CVE-2019-17564 and CVE-2021-25641 really turned out to be more of an… twitter.com/i/web/status/1…	2021-09-29 15:13:50

← Previous ID

Next ID→

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