



CVE-2021-31522

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

Summary

CVE	CVE-2021-31522
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-06 13:15:00 UTC
Updated	2022-01-12 20:52:00 UTC
Description	Kylin can receive user input and load any class through Class.forName(...). This issue affects Apache Kylin 2 version 2.6.6

Risk And Classification

Problem Types: CWE-470

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Kylin	All	All	All	All
Application	Apache	Kylin	4.0.0	-	All	All
Application	Apache	Kylin	4.0.0	alpha	All	All
Application	Apache	Kylin	4.0.0	beta	All	All
Application	Apache	Kylin	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - CVE-2021-31522: Apache Kylin unsafe class loading	MLIST	www.openwall.com	
lists.apache.org/thread/hh5crx3yr701zd8wtpqo1mww2rlkvzrw	MISC	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: bo yu <forhaby0@gmail.com>

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](#)