



CVE-2021-40146

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

Summary

CVE	CVE-2021-40146
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-11 11:15:00 UTC
Updated	2021-09-23 16:59:00 UTC
Description	A Remote Code Execution (RCE) vulnerability was discovered in the Any23 YAMLExtractor.java file and is known to affect .

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Any23	All	All	All	All

References

Reference	Source	Li
Pony Mail!	CONFIRM	lis
oss-security - CVE-2021-40146: A Remote Code Execution (RCE) vulnerability exists in Apache Any23 YAMLExtractor.java	MLIST	wn
CVE Program record	CVE.ORG	wn
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

LEGACY: The Apache Any23 Project Management Committee would like to thank Zhuxuan Wu for reporting the security vulnerability.

Legacy QID Mappings

[980670](#) Java (maven) Security Update for org.apache.any23:apache-any23 (GHSA-99px-7724-484v)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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