



CVE-2023-27602

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

Summary

CVE	CVE-2023-27602
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-10 08:15:00 UTC
Updated	2023-04-19 12:15:00 UTC
Description	In Apache Linkis <=1.3.1, The PublicService module uploads files without restrictions on the path to the uploaded files, and

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
oss-security - Re: CVE-2023-27602: Apache Linkis publicservice module unrestricted upload of file	MISC	www.openwall.com	
oss-security - CVE-2023-27602: Apache Linkis publicservice module unrestricted upload of file	MISC	www.openwall.com	Mailing List
lists.apache.org/thread/wt70jfc0yfs6s5g0wg5dr5klnc48nsp1	MISC	lists.apache.org	Mailing List
oss-security - Re: CVE-2023-27602: Apache Linkis publicservice module unrestricted upload of file	MISC	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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