



CVE-2020-17519

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

Summary

CVE	CVE-2020-17519
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-05 12:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	A change introduced in Apache Flink 1.11.0 (and released in 1.11.1 and 1.11.2 as well) allows attackers to read any file on

Risk And Classification

EPSS: 0.943310000 probability, percentile 0.999550000 (date 2026-05-15)

CISA KEV: Listed on 2024-05-23; due 2024-06-13; ransomware use Unknown

Problem Types: CWE-552

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Flink
Name	Apache Flink Improper Access Control Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://lists.apache.org/thread/typ0h03zyfrzjqlnb7plh64df1g2383d ; https://nvd.nist.gov/vuln/detail/CVE-2020-17519

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Pony Mail!		lists.apac
Pony Mail!	MLIST	lists.apac
Pony Mail!	MLIST	lists.apac

Pony Mail!	MLIS I	lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!		lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!	MISC	lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!		lists.apacl
Pony Mail!		lists.apacl
oss-security - [CVE-2020-17519] Apache Flink directory traversal attack: reading remote files through the REST API	MLIST	www.oper
Pony Mail!		lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!	MLIST	lists.apacl
Apache Flink 1.11.0 Arbitrary File Read / Directory Traversal ≈ Packet Storm	MISC	packetsto
Pony Mail!	MLIST	lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!		lists.apacl
Pony Mail!		lists.apacl
Pony Mail!		lists.apacl
Pony Mail!		lists.apacl
Pony Mail!	MISC	lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!		lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!	MLIST	lists.apacl
Pony Mail!		lists.apacl
Pony Mail!		lists.apacl
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa



Vendor Comments And Credit

Discovery Credit

LEGACY: 0rich1 of Ant Security FG Lab

Legacy QID Mappings

[730426](#) Apache Flink Arbitrary File Read Vulnerability

[982928](#) Java (maven) Security Update for org.apache.flink:flink-runtime_2.12 (GHSA-395w-qhqr-9fr6)

© [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](#)