Apache Kafka: Missing JWT token validation in OAUTHBEARER authentication

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-33557
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 14:16:18 UTC
Updated	2026-04-22 14:14:52 UTC
Description	A possible security vulnerability has been identified in Apache Kafka. By default, the broker property `sasl.oauthbearer.jwt.v

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

EPSS: 0.000430000 probability, percentile 0.132610000 (date 2026-04-22)

Problem Types: CWE-1285 | CWE-1285 CWE-1285 Improper Validation of Specified Index, Position, or Offset in Input

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Kafka	affected 4.1.0 4.1.1 semver	Not specified

References

Reference	Source	Link	Tags
lists.apache.org/thread/v57o00hm6yszdpdnvqx2ss4561yh953h	security@apache.org	lists.apache.org	Vendor A
kafka.apache.org/cve-list	security@apache.org	kafka.apache.org	Vendor A
www.openwall.com/lists/oss-security/2026/04/17/2	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing L
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

Vendor Comments And Credit

Discovery Credit

CNA: Павел Романов <promanov1994@gmail.com> (en)

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