XXE in esaml SAML library allows local file read and potential SSRF

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-28809
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 11:16:24 UTC
Updated	2026-04-06 17:17:09 UTC
Description	XML External Entity (XXE) vulnerability in esaml (and its forks) allows an attacker to cause the system to read local files an

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-611 | CWE-611 CWE-611 Improper Restriction of XML External Entity Reference

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

Low

ntegrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Dropbox	Esaml	Not specified	Not specified
CNA	Arekinath	Esaml	Not specified	Not specified
CNA	Handnot2	Esaml	Not specified	Not specified
CNA	Dropbox	Esaml	Not specified	Not specified
CNA	Jump-App	Esaml	affected bab85efde7c136911402a881ca55173759467a26 git	Not specified
CNA	Jump-App	Esaml	unaffected bab85efde7c136911402a881ca55173759467a26 git	Not specified

References

Reference	Source	Link
cna.erlef.org/cves/CVE-2026-28809.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erle
osv.dev/vulnerability/EEF-CVE-2026-28809	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
github.com/Jump-App/esaml/commit/bab85efde7c136911402a881ca55173759467a26	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Bryan Lynch (en)

CNA: Jonatan Männchen / EEF (en)

Additional Advisory Data

Workarounds

CNA: Upgrade to Erlang/OTP 27 or later. Starting with OTP 27, xmerl_scan disables entity expansion by default, which mitigates this vulnerability without changes to esaml.

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