



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

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

## Summary

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

## 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/MSX/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: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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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: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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

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/MSX: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	<a href="#">Dropbox</a>	<a href="#">Esaml</a>	Not specified	Not specified
CNA	<a href="#">Arekinath</a>	<a href="#">Esaml</a>	Not specified	Not specified
CNA	<a href="#">Handnot2</a>	<a href="#">Esaml</a>	Not specified	Not specified
CNA	<a href="#">Dropbox</a>	<a href="#">Esaml</a>	Not specified	Not specified
CNA	<a href="#">Jump-App</a>	<a href="#">Esaml</a>	affected bab85efde7c136911402a881ca55173759467a26 git	Not specified
CNA	<a href="#">Jump-App</a>	<a href="#">Esaml</a>	unaffected bab85efde7c136911402a881ca55173759467a26 git	Not specified

### References

Reference	Source	Link
<a href="https://cna.erlef.org/cves/CVE-2026-28809.html">cna.erlef.org/cves/CVE-2026-28809.html</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://cna.erlef.org/cves/CVE-2026-28809.html">cna.erlef.org</a>
<a href="https://osv.dev/vulnerability/EEF-CVE-2026-28809">osv.dev/vulnerability/EEF-CVE-2026-28809</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://osv.dev/vulnerability/EEF-CVE-2026-28809">osv.dev</a>
<a href="https://github.com/Jump-App/esaml/commit/bab85efde7c136911402a881ca55173759467a26">github.com/Jump-App/esaml/commit/bab85efde7c136911402a881ca55173759467a26</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://github.com/Jump-App/esaml/commit/bab85efde7c136911402a881ca55173759467a26">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### 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.

© [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](#).

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