Improper Restriction of XML External Entity Reference in Inkscape

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

Summary

CVE	CVE-2026-4980
State	PUBLISHED
Assigner	GitLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 15:17:03 UTC
Updated	2026-03-30 13:26:29 UTC
Description	A local file disclosure vulnerability in the XInclude processing component of Inkscape 1.1 before 1.3 allows a remote attacke

Risk And Classification

Primary CVSS: v3.1 6.3 MEDIUM from cve@gitlab.com

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

EPSS: 0.000270000 probability, percentile 0.076330000 (date 2026-04-06)

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

Version	Source	Type	Score	Severity	Vector
3.1	cve@gitlab.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	6.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Inkscape	Inkscape	affected 1.1 1.3 semver	Not specified

References

Reference	Source	Link	Tags
gitlab.com/inkscape/inkscape/-/merge_requests/5269	cve@gitlab.com	gitlab.com	
gitlab.com/inkscape/inkscape/-/work_items/3557	cve@gitlab.com	gitlab.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: VK (previously elttam) https://github.com/me0wday (en)

Additional Advisory Data

Solutions

CNA: Upgrade to version 1.3 or above

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 registred 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**