lxml: Default configuration of iterparse() and ETCompatXMLParser() allows XXE to local files

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

Summary

CVE	CVE-2026-41066
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 17:16:20 UTC
Updated	2026-04-27 17:59:05 UTC
Description	lxml is a library for processing XML and HTML in the Python language. Prior to 6.1.0, using either of the two parsers in the c

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security-advisories@github.com

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

EPSS: 0.000320000 probability, percentile 0.091000000 (date 2026-04-27)

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

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lxml	Lxml	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Lxml	Lxml	affected < 6.1.0	Not specified

References

Reference	Source	Link	Tags
github.com/lxml/lxml/security/advisories/GHSA-vfmq-68hx-4jfw	security-advisories@github.com	github.com	Mitigation, Vendor
bugs.launchpad.net/lxml/+bug/2146291	security-advisories@github.com	bugs.launchpad.net	Exploit, Issue Track
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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