Stack overflow in libxml2

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

Summary

CVE	CVE-2025-9714
State	PUBLISHED
Assigner	canonical
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-10 19:15:42 UTC
Updated	2026-05-12 13:17:30 UTC
Description	Uncontrolled recursion in XPath evaluation in libxml2 up to and including version 2.9.14 allows a local attacker to cause a s

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000090000 probability, percentile 0.009450000 (date 2026-05-12)

Problem Types: CWE-674 | CWE-674 CWE-674 Uncontrolled Recursion

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	security@ubuntu.com	Secondary	6.2	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.2	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xmlsoft	Libxml2	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Libxml2	Libxml2	affected 2.10.0 semver	Linux
CNA	Libxml2	Libxml2	affected 2.12.7+dfsg+really2.9.14-0.4ubuntu0.3 dpkg	Linux
CNA	Libxml2	Libxml2	affected 2.9.14+dfsg-1.3ubuntu3.5 dpkg	Linux
CNA	Libxml2	Libxml2	affected 2.9.13+dfsg-1ubuntu0.9 dpkg	Linux
CNA	Libxml2	Libxml2	affected 2.9.10+dfsg-5ubuntu0.20.04.10+esm2 dpkg	Linux
CNA	Libxml2	Libxml2	affected 2.9.4+dfsg1-6.1ubuntu1.9+esm5 dpkg	Linux
CNA	Libxml2	Libxml2	affected 2.9.3+dfsg1-1ubuntu0.7+esm10 dpkg	Linux
CNA	Libxml2	Libxml2	affected 2.9.1+dfsg1-3ubuntu4.13+esm9 dpkg	Linux
ADP	Siemens	RUGGEDCOM ROX MX5000	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX MX5000RE	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1400	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1500	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1501	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1510	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1511	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1512	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1524	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1536	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX5000	affected V2.17.1 custom	Not specified

References

Reference	Source	Li
gitlab.gnome.org/GNOME/libxml2/-/commit/677a42645ef22b5a50741bad5facf9d8a8bc6d21	security@ubuntu.com	gi
lists.debian.org/debian-lts-announce/2025/09/msg00035.html	af854a3a-2127-422b-91ae-364da2661108	lis
cert-portal.siemens.com/productcert/html/ssa-577017.html	0b142b55-0307-4e5a-b3e0-f314f2fb7e5e	ce

cert-portal.siemens.com/productcert/html/ssa-577017.html	0b142b55-0307-4c5a-b3c9-1314f3fb7c5e	ce
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

CNA: Nikita Sveshnikov (Positive Technologies) (en)

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