Libxml: type confusion leads to denial of service (dos)

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

Summary

CVE	CVE-2025-49796
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-16 16:15:19 UTC
Updated	2026-04-19 20:16:21 UTC
Description	A vulnerability was found in libxml2. Processing certain sch:name elements from the input XML file can trigger a memory cc

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from secalert@redhat.com

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

EPSS: 0.017770000 probability, percentile 0.827210000 (date 2026-04-19)

Problem Types: CWE-125 | CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:2.12.5-7.el10_0 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:2.9.1-6.el7_9.10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.9.7-21.el8_10.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.9.7-21.el8_10.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:2.9.7-9.el8_2.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:2.9.7-9.el8_4.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:2.9.7-9.el8_4.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:2.9.7-13.el8_6.10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:2.9.7-13.el8_6.10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:2.9.7-13.el8_6.10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:2.9.7-16.el8_8.9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:2.9.7-16.el8_8.9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.9.13-10.el9_6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.9.13-10.el9_6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:2.9.13-1.el9_0.5 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:2.9.13-3.el9_2.7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:2.9.13-10.el9_4 * rpm
CNA	Red Hat	Red Hat JBoss Core Services 2.4.62.SP2	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4.12	unaffected 412.86.202510291903-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.13	unaffected 413.92.202510150118-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.14	unaffected 414.92.202510211419-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.17	unaffected 417.94.202510112152-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.18	unaffected 418.94.202510230424-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.19	unaffected 4.19.9.6.202510140714-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.20	unaffected 4.20.9.6.202509251656-0 * rpm
CNA	Red Hat	Red Hat Web Terminal 1.11 On RHEL 9	unaffected 1.11-19 * rpm
CNA	Red Hat	Red Hat Web Terminal 1.11 On RHEL 9	unaffected 1.11-8 * rpm
CNA	Red Hat	Red Hat Web Terminal 1.12 On RHEL 9	unaffected 1.12-4 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-11 * rpm

CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-11 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-11 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-10 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-10 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-4 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-9 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-18 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-11 * rpm
CNA	Red Hat	RHOSS-1.36-RHEL-8	unaffected 1.36.0-7 * rpm
CNA	Red Hat	Cert-manager Operator For Red Hat OpenShift 1.16	unaffected sha256:1abdfac084e7c86e7a93
CNA	Red Hat	File Integrity Operator 1	unaffected sha256:364d11af112a5b1d3f28
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:ad07f55ee75fb20310c88
CNA	Red Hat	Red Hat Hardened Images	unaffected 2.15.2-0.3.hum1 * rpm
CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:c26d589f12647890b67a
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2025:21913	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:18217	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7519	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0934	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:11580	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:10698	secalert@redhat.com	access.redhat.com	
gitlab.gnome.org/GNOME/libxml2/-/issues/933	secalert@redhat.com	gitlab.gnome.org	
access.redhat.com/errata/RHSA-2025:12241	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:10699	secalert@redhat.com	access.redhat.com	
lists.debian.org/debian-lts-announce/2025/07/msg00014.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/errata/RHSA-2025:12240	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:12199	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:18219	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:10630	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19041	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:18218	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19894	secalert@redhat.com	access.redhat.com	

access.redhat.com/errata/RHSA-2025:13335	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-49796	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:12239	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2025:19046	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:19020	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:18240	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:15828	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:15397	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:12098	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:12237	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:15827	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:13267	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:12099	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-06-12T00:35:26.470Z	Reported to Red Hat.
CNA	2025-06-11T00:00:00.000Z	Made public.

Workarounds

CNA: There's no available mitigation other than to avoid processing untrusted XML documents if the user is unable/unwilling to update the library.

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

CVE.report and Source URL Uptime Status status.cve.report