Libxml: null pointer dereference leads to denial of service (dos)

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

Summary

CVE	CVE-2025-49795
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 NULL pointer dereference vulnerability was found in libxml2 when processing XPath XML expressions. This flaw allows a

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert@redhat.com

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

EPSS: 0.005660000 probability, percentile 0.684980000 (date 2026-04-19)

Problem Types: CWE-825 | CWE-825 Expired Pointer Dereference

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:2.12.5-7.el10_0 * rpm	Not specified
CNA	Red Hat	Red Hat JBoss Core Services 2.4.62.SP2	Not specified	Not specified
CNA	Red Hat	Red Hat Hardened Images	unaffected 2.15.2-0.3.hum1 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:7519	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2025-49795	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:10630	secalert@redhat.com	access.redhat.com	
gitlab.gnome.org/GNOME/libxml2/-/issues/932	secalert@redhat.com	gitlab.gnome.org	
access.redhat.com/errata/RHSA-2025:19020	secalert@redhat.com	access.redhat.com	
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.

Additional Advisory Data

Source	Time	Event
CNA	2025-06-12T00:31:08.194Z	Reported to Red Hat.
CNA	2025-06-11T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation is either unavailable or does not meet Red Hat Product Security standards for usability, deployment, applicability, or stability.

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

Free CVE JSON API cve.report/api

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