Libxml2: stack buffer overflow in xmllint interactive shell command handling

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

Summary

CVE	CVE-2025-6170
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-16 16:15:20 UTC
Updated	2026-04-19 20:16:22 UTC
Description	A flaw was found in the interactive shell of the xmllint command-line tool, used for parsing XML files. When a user inputs an

Risk And Classification

Primary CVSS: v3.1 2.5 LOW from nvd@nist.gov

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

EPSS: 0.001180000 probability, percentile 0.306270000 (date 2026-04-19)

Problem Types: CWE-121 | CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L
3.1	secalert@redhat.com	Secondary	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

None

vailability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Jboss Core Services	-	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Xmlsoft	Libxml2	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Hardened Images	unaffected 2.15.2-0.3.hum1 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	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
CNA	Red Hat	Red Hat JBoss Core Services	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	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	Issue Trac
lists.debian.org/debian-lts-announce/2025/07/msg00014.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/security/cve/CVE-2025-6170	secalert@redhat.com	access.redhat.com	Mitigation,
gitlab.gnome.org/GNOME/libxml2/-/issues/941	secalert@redhat.com	gitlab.gnome.org	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Ahmed Lekssays for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-06-16T05:33:22.955Z	Reported to Red Hat.
CNA	2025-06-16T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to a widespread installation base, or stability. It is strongly recommended to apply the upstream patch once available.

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