Libxml2: integer overflow in xmlbuildqname() leads to stack buffer overflow in libxml2

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

Summary

CVE	CVE-2025-6021
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-12 13:15:25 UTC
Updated	2026-04-19 20:16:22 UTC
Description	A flaw was found in libxml2's xmlBuildQName function, where integer overflows in buffer size calculations can lead to a stac

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: 0.021160000 probability, percentile 0.841470000 (date 2026-04-19)

Problem Types: CWE-787 | CWE-787 Out-of-bounds Write

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Redhat	Enterprise Linux	10.0	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux	9.0	All
Operating System	Redhat	Enterprise Linux Eus	10.0	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All
Operating System	Redhat	Enterprise Linux Eus	8.8	All
Operating System	Redhat	Enterprise Linux Eus	9.4	All
Operating System	Redhat	Enterprise Linux Eus	9.6	All
Operating System	Redhat	Enterprise Linux For Arm 64	10.0_aarch64	All
Operating System	Redhat	Enterprise Linux For Arm 64	8.0_aarch64	All
Operating System	Redhat	Enterprise Linux For Arm 64	9.0_aarch64	All
Operating System	Redhat	Enterprise Linux For Arm 64	9.4_aarch64	All
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	10.0_aarch64	All
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	9.4_aarch64	All
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	9.6_aarch64	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	10.0_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	9.4_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	10.0_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	9.0_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	9.4_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	9.6_s390x	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	10.0_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.0_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	10.0_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	9.4_ppc64le	All

Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	9.6_ppc64le	All
Operating System	Redhat	Enterprise Linux Server	7.0	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All
Operating System	Redhat	Enterprise Linux Server Aus	9.2	All
Operating System	Redhat	Enterprise Linux Server Aus	9.4	All
Operating System	Redhat	Enterprise Linux Server Aus	9.6	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	9.4_ppc64le	All
Operating System	Redhat	Enterprise Linux Server Tus	8.8	All
Operating System	Redhat	In-vehicle Operating System	1.0	All
Application	Redhat	Jboss Core Services	-	All
Application	Redhat	Openshift Container Platform	4.12	All
Application	Redhat	Openshift Container Platform	4.13	All
Application	Redhat	Openshift Container Platform	4.14	All
Application	Redhat	Openshift Container Platform	4.15	All
Application	Redhat	Openshift Container Platform	4.16	All
Application	Redhat	Openshift Container Platform	4.17	All
Application	Redhat	Openshift Container Platform	4.18	All
Application	Redhat	Openshift Container Platform For Arm64	4.13	All
Application	Redhat	Openshift Container Platform For Arm64	4.14	All
Application	Redhat	Openshift Container Platform For Arm64	4.15	All
Application	Redhat	Openshift Container Platform For Arm64	4.16	All
Application	Redhat	Openshift Container Platform For Arm64	4.17	All
Application	Redhat	Openshift Container Platform For Arm64	4.18	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.13	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.14	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.15	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.16	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.17	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.18	All
Application	Redhat	Openshift Container Platform For Linuxone	4.13	All
Application	Redhat	Openshift Container Platform For Linuxone	4.14	All
Application	Redhat	Openshift Container Platform For Linuxone	4.15	All
Application	Redhat	Openshift Container Platform For Linuxone	4.16	All

Application	Redhat	Openshift Container Platform For Linuxone	4.17	All
Application	Redhat	Openshift Container Platform For Linuxone	4.18	All
Application	Redhat	Openshift Container Platform For Power	4.13	All
Application	Redhat	Openshift Container Platform For Power	4.14	All
Application	Redhat	Openshift Container Platform For Power	4.15	All
Application	Redhat	Openshift Container Platform For Power	4.16	All
Application	Redhat	Openshift Container Platform For Power	4.17	All
Application	Redhat	Openshift Container Platform For Power	4.18	All
Application	Xmlsoft	Libxml2	All	All

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 412.86.202509030110-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.13	unaffected 413.92.202509030117-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.14	unaffected 414.92.202508041909-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.15	unaffected 415.92.202508192014-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.16	unaffected 416.94.202508050040-0 * rpm

CNA	Red Hat	Red Hat OpenShift Container Platform 4.17	unaffected 417.94.202508141510-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.18	unaffected 418.94.202508060022-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.19	unaffected 4.19.9.6.202507230107-0 * rpm
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:ad07f55ee75fb20310c8
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-2026:7519	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:11580	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:10698	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:12241	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:13336	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:15672	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:10699	secalert@redhat.com	access.redhat.com	Third Party
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	Third Party
access.redhat.com/errata/RHSA-2025:12199	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:10630	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:13335	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:14059	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/security/cve/CVE-2025-6021	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:12239	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:19020	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:13325	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:15308	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:12098	secalert@redhat.com	access.redhat.com	Third Party
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Trac
gitlab.gnome.org/GNOME/libxml2/-/issues/926	134c704f-9b21-4f2e-91b3-4a467353bcc0	gitlab.gnome.org	Exploit, Iss
access.redhat.com/errata/RHSA-2025:12237	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:11673	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:14396	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:13267	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2025:13289	secalert@redhat.com	access.redhat.com	Third Party

access.redhat.com/errata/RHSA-2025:12099	secalert@redhat.com	access.redhat.com	Third Party
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	2025-06-12T07:55:45.428Z	Reported to Red Hat.
CNA	2025-06-12T00:00:00.000Z	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 widespread installation base, or stability. Users are strongly advised to apply vendor-supplied patches as soon as they become available to address the underlying integer overflow flaw in the affected code.

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