Libxslt: heap use-after-free in libxslt caused by atype corruption in xmlattrptr

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

Summary

CVE	CVE-2025-7425
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-10 14:15:27 UTC
Updated	2026-04-14 22:16:28 UTC
Description	A flaw was found in libxslt where the attribute type, atype, flags are modified in a way that corrupts internal memory manage

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from secalert@redhat.com

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

EPSS: 0.000610000 probability, percentile 0.189060000 (date 2026-04-15)

Problem Types: CWE-416 | CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	GNOME	Libxml2	affected 2.15.2 semver
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:2.12.5-8.el10_0 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:1.1.39-8.el10_0 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:2.9.1-6.el7_9.12 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.9.7-21.el8_10.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.9.7-21.el8_10.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:2.9.7-9.el8_2.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:2.9.7-9.el8_4.7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:2.9.7-9.el8_4.7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:2.9.7-13.el8_6.11 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:2.9.7-13.el8_6.11 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:2.9.7-13.el8_6.11 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:2.9.7-16.el8_8.10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:2.9.7-16.el8_8.10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.9.13-11.el9_6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.9.13-11.el9_6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:2.9.13-1.el9_0.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:2.9.13-3.el9_2.8 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:2.9.13-11.el9_4 * rpm
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 414.92.202508270040-0 * 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 416.94.202508261955-0 * 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 418.94.202508261658-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.19	unaffected 4.19.9.6.202508271124-0 * 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	Compliance Operator 1	unaffected sha256:4953a7ea865ff38a4fe19
CNA	Red Hat	Compliance Operator 1	unaffected sha256:06ad8599c4b0170264e
CNA	Red Hat	Compliance Operator 1	unaffected sha256:0903a7a5c857d96c84fc
CNA	Red Hat	File Integrity Operator 1	unaffected sha256:364d11af112a5b1d3f28
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:ad07f55ee75fb20310c8
CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:c26d589f12647890b67a
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:2a359b16651cf20b9e37
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:02d88da5fdc965b3759b
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:260572b783d27d50a2d
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:783a10c95edcb5c5cb83
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:39b2d56b8f0eb3b53969
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:0932824cfd76c0e3d80f
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:264613b2add0f32e5f53
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:2509c7cc0bdf6d001442
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.5.1	unaffected sha256:c6f9ee5f306766c05024
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Hardened Images	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-2026:0934	secalert@redhat.com	access.redhat.com	

seclists.org/fulldisclosure/2025/Jul/32	af854a3a-2127-422b-91ae-364da2661108	seclists.org
access.redhat.com/errata/RHSA-2025:14853	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13314	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13622	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:15672	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:21885	secalert@redhat.com	access.redhat.com
www.openwall.com/lists/oss-security/2025/07/11/2	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
access.redhat.com/errata/RHSA-2025:14819	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:18219	secalert@redhat.com	access.redhat.com
gitlab.gnome.org/GNOME/libxslt/-/issues/140	134c704f-9b21-4f2e-91b3-4a467353bcc0	gitlab.gnome.org
seclists.org/fulldisclosure/2025/Jul/37	af854a3a-2127-422b-91ae-364da2661108	seclists.org
seclists.org/fulldisclosure/2025/Aug/0	af854a3a-2127-422b-91ae-364da2661108	seclists.org
access.redhat.com/errata/RHSA-2025:13335	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:14818	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHBA-2025:12345	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:14059	secalert@redhat.com	access.redhat.com
lists.debian.org/debian-lts-announce/2025/09/msg00035.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
access.redhat.com/errata/RHSA-2025:13311	secalert@redhat.com	access.redhat.com
access.redhat.com/security/cve/CVE-2025-7425	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13310	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:12447	secalert@redhat.com	access.redhat.com
seclists.org/fulldisclosure/2025/Jul/35	af854a3a-2127-422b-91ae-364da2661108	seclists.org
access.redhat.com/errata/RHSA-2025:12450	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:15308	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:15828	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13464	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13308	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13313	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:14858	secalert@redhat.com	access.redhat.com
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com
access.redhat.com/errata/RHSA-2025:15827	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:14396	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13267	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:13309	secalert@redhat.com	access.redhat.com
seclists.org/fulldisclosure/2025/Jul/30	af854a3a-2127-422b-91ae-364da2661108	seclists.org

access.redhat.com/errata/RHSA-2025:13312	secalert@redhat.com	access.redhat.com	
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 Sergei Glazunov (Google Project Zero) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-07-10T09:37:28.172Z	Reported to Red Hat.
CNA	2025-07-10T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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