Libxslt: type confusion in xmlnode.psvi between stylesheet and source nodes

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

Summary

CVE	CVE-2025-7424
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 22:16:27 UTC
Description	A flaw was found in the libxslt library. The same memory field, psvi, is used for both stylesheet and input data, which can le

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.000880000 probability, percentile 0.251900000 (date 2026-04-15)

Problem Types: CWE-843 | CWE-843 Access of Resource Using Incompatible Type ('Type Confusion')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	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	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

Integrity

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	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	Openshift Container Platform	4.0	All	All	All
Application	Xmlsoft	Libxslt	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GNOME	Libxslt	affected 1.1.44 semver	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:2.12.5-8.el10_0 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:1.1.39-8.el10_0 * 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
CNA	Red Hat	Red Hat Hardened Images	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/security/cve/CVE-2025-7424	secalert@redhat.com	access.redhat.com	Third Party
seclists.org/fulldisclosure/2025/Jul/32	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
www.openwall.com/lists/oss-security/2025/07/11/2	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
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	

seclists.org/fulldisclosure/2025/Jul/33	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
access.redhat.com/errata/RHBA-2025:12345	secalert@redhat.com	access.redhat.com	
seclists.org/fulldisclosure/2025/Jul/35	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
lists.debian.org/debian-lts-announce/2025/09/msg00024.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Trac
gitlab.gnome.org/GNOME/libxslt/-/issues/139	secalert@redhat.com	gitlab.gnome.org	
seclists.org/fulldisclosure/2025/Jul/30	af854a3a-2127-422b-91ae-364da2661108	seclists.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 Ivan Fratric (Google Project Zero) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-07-10T08:34:02.563Z	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.