



# CVE-2017-5969

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-5969
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-11 16:59:00 UTC
<b>Updated</b>	2023-11-07 02:49:00 UTC
<b>Description</b>	** DISPUTED ** libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dereference) by parsing a crafted XML file.

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xmlsoft	Libxml2	2.9.4	All	All	All
Application	Xmlsoft	Libxml2	2.9.4	All	All	All

## References

Reference	Source	Link
oss-security - CVE request: Null pointer dereference parsing xml file using libxml 2.9.4 (in recover mode)	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
[SECURITY] [DLA 2972-1] libxml2 security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>
libxml2: Multiple vulnerabilities (GLSA 201711-01) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
oss-security - CVE-2017-5969: Null pointer dereference parsing xml file using libxml 2.9.4 (in recover mode)	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
libxml2 CVE-2017-5969 Null Pointer Dereference Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Bug 778519 – CVE-2017-5969: null pointer dereference when parsing a xml file using recover mode	MISC	<a href="http://bugzilla.gnome.org">bugzilla.gnome.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[179176](#) Debian Security Update for libxml2 (DLA 2972-1)

[500348](#) Alpine Linux Security Update for libxml2

[504111](#) Alpine Linux Security Update for libxml2

[710359](#) Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 201711-01)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**