



# CVE-2018-14567

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-14567
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-16 20:29:00 UTC
<b>Updated</b>	2020-09-10 01:15:00 UTC
<b>Description</b>	libxml2 2.9.8, if --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via a crafted XML file

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.9.8	All	All	All
Application	<a href="#">Xmlsoft</a>	<a href="#">Libxml2</a>	2.9.8	All	All	All

## References

Reference	Source	Link	Tags
Fix infinite loop in LZMA decompression (2240fbf5) · Commits · GNOME / libxml2 · GitLab	CONFIRM	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>	Patch, Thi
[SECURITY] [DLA 2369-1] libxml2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
libxml2 CVE-2018-14567 Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Part
USN-3739-1: libxml2 vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Part

[SECURITY] [DLA 1524-1] libxml2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Third Part
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [377223](#) Alibaba Cloud Linux Security Update for libxml2 (ALINUX2-SA-2020:0077)
- [500349](#) Alpine Linux Security Update for libxml2
- [504112](#) Alpine Linux Security Update for libxml2
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

© [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](#)**