



# CVE-2021-28906

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-28906
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-20 19:15:00 UTC
<b>Updated</b>	2022-04-06 17:35:00 UTC
<b>Description</b>	In function read_yin_leaf() in libyang <= v1.0.225, it doesn't check whether the value of retval->ext[r] is NULL. In some case

## Risk And Classification

**Problem Types:** CWE-252

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cesnet	Libyang	All	All	All	All

## References

### Reference

- libyang: Multiple vulnerabilities (GLSA 202107-54) — Gentoo security
- In function "read\_yin\_leaf", the value "retval->ext[r]" can be NULL. The operation "retval->ext[r]->flags" result in a crash · Issue #1455 · CESNET/libyang
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 501614 Alpine Linux Security Update for libyang
- 501878 Alpine Linux Security Update for libyang
- 710041 Gentoo Linux libyang Multiple Vulnerabilities (GLSA 202107-54)
- 753130 SUSE Enterprise Linux Security Update for libyang (SUSE-SU-2022:3245-1)

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

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