



# CVE-2019-20391

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

## Summary

<b>CVE</b>	CVE-2019-20391
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-22 22:15:00 UTC
<b>Updated</b>	2023-09-19 22:15:00 UTC
<b>Description</b>	An invalid memory access flaw is present in libyang before v1.0-r3 in the function resolve_feature_value() when an if-featur

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cesnet	Libyang	0.11	r1	All	All
Application	Cesnet	Libyang	0.11	r2	All	All
Application	Cesnet	Libyang	0.12	r1	All	All
Application	Cesnet	Libyang	0.12	r2	All	All
Application	Cesnet	Libyang	0.13	r1	All	All
Application	Cesnet	Libyang	0.13	r2	All	All
Application	Cesnet	Libyang	0.14	r1	All	All
Application	Cesnet	Libyang	0.15	r1	All	All
Application	Cesnet	Libyang	0.16	r1	All	All
Application	Cesnet	Libyang	0.16	r2	All	All
Application	Cesnet	Libyang	0.16	r3	All	All
Application	Cesnet	Libyang	1.0	r1	All	All
Application	Cesnet	Libyang	1.0	r2	All	All
Application	Cesnet	Libyang	0.11	r1	All	All
Application	Cesnet	Libyang	0.11	r2	All	All
Application	Cesnet	Libyang	0.12	r1	All	All
Application	Cesnet	Libyang	0.12	r2	All	All

Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.13	r1	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.13	r2	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.14	r1	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.15	r1	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.16	r1	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.16	r2	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.16	r3	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	1.0	r1	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	1.0	r2	All	All

## References

### Reference

resolve BUGFIX handle yet unresolved if-features · CESNET/libyang@bdb596d · GitHub

Segmentation fault in yangfuzz and yanglint · Issue #772 · CESNET/libyang · GitHub

[SECURITY] [DLA 3572-1] libyang security update

1793934 – (CVE-2019-20391) CVE-2019-20391 libyang: invalid memory access in resolve\_feature\_value() when a if-feature is used inside a l

Comparing v1.0-r2...v1.0-r3 · CESNET/libyang · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[6000044](#) Debian Security Update for libyang (DLA 3572-1)

© [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](#)