



# CVE-2019-19334

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

## Summary

<b>CVE</b>	CVE-2019-19334
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-06 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:07:00 UTC
<b>Description</b>	In all versions of libyang before 1.0-r5, a stack-based buffer overflow was discovered in the way libyang parses YANG files

## Risk And Classification

**Problem Types:** CWE-787

## 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	1.0	r3	All	All
Application	Cesnet	Libyang	1.0	r4	All	All
Application	Cesnet	Libyang	0.11	r1	All	All
Application	Cesnet	Libyang	0.11	r2	All	All

Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	0.12	r1	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	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
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	1.0	r3	All	All
Application	<a href="#">Cesnet</a>	<a href="#">Libyang</a>	1.0	r4	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

## References

### Reference

1779576 – (CVE-2019-19334) CVE-2019-19334 libyang: stack-based buffer overflow in make_canonical when identityref leaf type is used	C
[SECURITY] Fedora 31 Update: libyang-1.0.101-1.fc31 - package-announce - Fedora Mailing-Lists	F
parser BUGFIX long identityref default value buffer overflow · CESNET/libyang@6980afa · GitHub	C
[SECURITY] Fedora 31 Update: libyang-1.0.101-1.fc31 - package-announce - Fedora Mailing-Lists	F
[SECURITY] Fedora 30 Update: libyang-1.0.101-1.fc30 - package-announce - Fedora Mailing-Lists	F
Red Hat Customer Portal	F
[SECURITY] Fedora 30 Update: libyang-1.0.101-1.fc30 - package-announce - Fedora Mailing-Lists	F
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[377141](#) Alibaba Cloud Linux Security Update for libyang (ALINUX3-SA-2022:0076)

[940066](#) AlmaLinux Security Update for libyang (ALSA-2019:4360)

© [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](#)