



# CVE-2018-20857

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

## Summary

<b>CVE</b>	CVE-2018-20857
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-26 12:15:00 UTC
<b>Updated</b>	2019-08-01 16:59:00 UTC
<b>Description</b>	Zendesk Samlr before 2.6.2 allows an XML nodes comment attack such as a name_id node with user@example.com follow

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Zendesk</a>	<a href="#">Samlr</a>	All	All	All	All
Application	<a href="#">Zendesk</a>	<a href="#">Samlr</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Comparing v2.6.1...v2.6.2 · zendesk/samlr · GitHub	MISC	<a href="#">github.com</a>	Patch, Third Party Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**