



# CVE-2022-43358

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

## Summary

<b>CVE</b>	CVE-2022-43358
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-22 19:16:00 UTC
<b>Updated</b>	2023-08-30 19:34:00 UTC
<b>Description</b>	Stack overflow vulnerability in ast_selectors.cpp: in function Sass::ComplexSelector::has_placeholder in libsass:3.6.5-8-g21

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sass-lang	Libsass	3.6.5-8-g210218	All	All	All

## References

### Reference

- AddressSanitizer: stack-overflow src/ast\_selectors.cpp:464 in Sass::ComplexSelector::has\_placeholder() const · Issue #3178 · sass/libsass · C
- GitHub - sass/libsass: A C/C++ implementation of a Sass compiler
- poc3 - Google Drive
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 506111 Alpine Linux Security Update for libsass
- 755484 SUSE Enterprise Linux Security Update for libsass (SUSE-SU-2023:4895-1)
- 755485 SUSE Enterprise Linux Security Update for libsass (SUSE-SU-2023:4895-1)

© [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](#)