



# CVE-2018-25047

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

## Summary

<b>CVE</b>	CVE-2018-25047
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-15 00:15:00 UTC
<b>Updated</b>	2023-03-03 20:00:00 UTC
<b>Description</b>	In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty_fur

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Smarty</a>	<a href="#">Smarty</a>	All	All	All	All
Application	<a href="#">Smarty</a>	<a href="#">Smarty</a>	All	All	All	All

## References

Reference	Source	Link
Release v3.1.47 · smarty-php/smarty · GitHub	MISC	<a href="#">github.com</a>
smarty_function_mailto - JavaScript injection in eval function · Issue #454 · smarty-php/smarty · GitHub	MISC	<a href="#">github.com</a>
870100 – (CVE-2018-25047) <dev-php/smarty-4.2.1: javascript injection in mailto function	MISC	<a href="#">bugs.gentoo.org</a>
[SECURITY] [DLA 3262-1] smarty3 security update	MLIST	<a href="#">lists.debian.org</a>
Smarty: Multiple vulnerabilities (GLSA 202209-09) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
Release v4.2.1 · smarty-php/smarty · GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[181460](#) Debian Security Update for smarty3 (DLA 3262-1)

[710622](#) Gentoo Linux Smarty Multiple Vulnerabilities (GLSA 202209-09)

© [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](#).

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