



CVE-2021-44118

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-44118
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-26 12:15:00 UTC
Updated	2022-02-01 19:46:00 UTC
Description	SPiP 4.0.0 is affected by a Cross Site Scripting (XSS) vulnerability. To exploit the vulnerability, a visitor must browse to a m

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spip	Spip	4.0.0	All	All	All

References

Reference

- Quand on fait une copie locale d'une image pour la filtrer ensuite, ne pas oublier de passer un coup de sanitizer si besoin - 4ccf90a691 - spip ·
- Quand on ajoute un document distant ne pas perdre la trace de la copie_locale eventuellement faite au passage, l'utiliser pour avoir les infos c
- Refactoring de distant : · 1cf91def15 - spip - SPIP on GIT
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [183219](#) Debian Security Update for spip (CVE-2021-44118)
- [198833](#) Ubuntu Security Notification for SPIP Vulnerabilities (USN-5482-1)
- [199203](#) Ubuntu Security Notification for SPIP Vulnerabilities (USN-5482-2)

© [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](#)