



# CVE-2023-27372

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

## Summary

<b>CVE</b>	CVE-2023-27372
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-28 20:15:00 UTC
<b>Updated</b>	2023-06-21 18:15:00 UTC
<b>Description</b>	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. Th

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Spip	Spip	All	All	All	All
Application	Spip	Spip	4.2.0	-	All	All
Application	Spip	Spip	4.2.0	alpha	All	All
Application	Spip	Spip	4.2.0	alpha2	All	All

## References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-5367-1 spip	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
Fix: Sanitizer toutes les valeurs passées aux formulaires - 96fbeb3871 - spip - SPIP on GIT	MISC	<a href="https://git.spip.net">git.spip.net</a>	
Mise à jour critique de sécurité : sortie de SPIP 4.2.1, SPIP 4.1.8, SPIP (...) - SPIP Blog	MISC	<a href="https://blog.spip.net">blog.spip.net</a>	
SPIP Remote Command Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
Fix: Sanitizer toutes les valeurs passées aux formulaires - 5aedf49b89 - spip - SPIP on GIT	MISC	<a href="https://git.spip.net">git.spip.net</a>	
SPIP 4.2.1 Remote Code Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[181621](#) Debian Security Update for spip (DLA 3347-2)

[181669](#) Debian Security Update for spip (DSA 5367-1)

[183010](#) Debian Security Update for spip (CVE-2023-27372)

© [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](#)