



CVE-2021-44123

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-44123 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-01-26 12:15:00 UTC |
| Updated | 2022-02-02 16:15:00 UTC |
| Description | SPIP 4.0.0 is affected by a remote command execution vulnerability. To exploit the vulnerability, an attacker must craft a m... |

Risk And Classification

Problem Types: CWE-434

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 | Source | Link | Tags |
|--|---------|---|---------------------|
| Refactoring de distant : · 1cf91def15 - spip - SPIP on GIT | MISC | git.spip.net | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [183070](#) Debian Security Update for spip (CVE-2021-44123)
- [198833](#) Ubuntu Security Notification for SPIP Vulnerabilities (USN-5482-1)
- [199203](#) Ubuntu Security Notification for SPIP Vulnerabilities (USN-5482-2)

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](#)