



CVE-2013-7303

Published on: 01/30/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7303

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: PDF



Certain versions of [Spip](#) from [Spip](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in (1) squelettes-dist/formulaires/inscription.php and (2) prive/forms/editer_auteur.php in SPIP before 2.1.25 and 3.0.x before 3.0.13 allow remote attackers to inject arbitrary web script or HTML via the author name field.

CVE-2013-7303 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Changements entre 3.0.11 et 3.0.13 - SPIP

[www.spip.net](#)
[text/html](#)

[CONFIRM www.spip.net/fr_article5648.html](#)

oss-sec: Re: CVE request: spip: cross-site scripting vulnerability

[seclists.org](#)
[text/html](#)

[MLIST \[oss-security\] 20140120 Re: CVE request: spip: cross-site scripting vulnerability](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF spip-cve20137303-xss\(90643\)](#)

Security Advisory SA56381 - SPIP Author Page Name Script Insertion Vulnerability - Secunia

[web.archive.org](#)
[text/html](#)

[SECUNIA 56381](#)

Révision 20902 - ecrire/inc/filtres.php, prive/formulaires/editer_auteur.php : éviter un xss s... - SPIP - SPIP Core (Forge de développement)

[core.spip.org](#)
[text/html](#)

[CONFIRM core.spip.org/projects/spip/repository/revisions/20902](#)

oss-sec: CVE request: spip: cross-site scripting

[seclists.org](#)

[MLIST \[oss-security\] 20140120 CVE request:](#)

vulnerability	text/html	spip: cross-site scripting vulnerability
SPIP Input Validation Flaw in Author Name Field Permits Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1029703
Changements entre 2.1.24 et 2.1.25 - SPIP	www.spip.net text/html	 CONFIRM www.spip.net/fr_article5665.html
Changeset 77768 – SPIP-ZONE	zone.spip.org text/html	 CONFIRM zone.spip.org/trac/spip-zone/changeset/77768

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Spip	Spip	2.0.1	All	All	All
Application	Spip	Spip	2.0.10	All	All	All
Application	Spip	Spip	2.0.11	All	All	All
Application	Spip	Spip	2.0.12	All	All	All
Application	Spip	Spip	2.0.13	All	All	All
Application	Spip	Spip	2.0.14	All	All	All
Application	Spip	Spip	2.0.15	All	All	All
Application	Spip	Spip	2.0.16	All	All	All
Application	Spip	Spip	2.0.17	All	All	All
Application	Spip	Spip	2.0.18	All	All	All
Application	Spip	Spip	2.0.19	All	All	All
Application	Spip	Spip	2.0.2	All	All	All
Application	Spip	Spip	2.0.20	All	All	All
Application	Spip	Spip	2.0.21	All	All	All
Application	Spip	Spip	2.0.22	All	All	All
Application	Spip	Spip	2.0.3	All	All	All
Application	Spip	Spip	2.0.4	All	All	All
Application	Spip	Spip	2.0.5	All	All	All
Application	Spip	Spip	2.0.6	All	All	All
Application	Spip	Spip	2.0.7	All	All	All
Application	Spip	Spip	2.0.8	All	All	All
Application	Spip	Spip	2.0.9	All	All	All

Application	Spip	Spip	2.0.0	All	All	All
Application	Spip	Spip	2.1	All	All	All
Application	Spip	Spip	2.1.1	All	All	All
Application	Spip	Spip	2.1.10	All	All	All
Application	Spip	Spip	2.1.11	All	All	All
Application	Spip	Spip	2.1.12	All	All	All
Application	Spip	Spip	2.1.13	All	All	All
Application	Spip	Spip	2.1.14	All	All	All
Application	Spip	Spip	2.1.15	All	All	All
Application	Spip	Spip	2.1.16	All	All	All
Application	Spip	Spip	2.1.17	All	All	All
Application	Spip	Spip	2.1.18	All	All	All
Application	Spip	Spip	2.1.19	All	All	All
Application	Spip	Spip	2.1.2	All	All	All
Application	Spip	Spip	2.1.20	All	All	All
Application	Spip	Spip	2.1.21	All	All	All
Application	Spip	Spip	2.1.22	All	All	All
Application	Spip	Spip	2.1.23	All	All	All
Application	Spip	Spip	3.0.0	All	All	All
Application	Spip	Spip	3.0.1	All	All	All
Application	Spip	Spip	3.0.10	All	All	All
Application	Spip	Spip	3.0.11	All	All	All
Application	Spip	Spip	3.0.2	All	All	All
Application	Spip	Spip	3.0.3	All	All	All
Application	Spip	Spip	3.0.4	All	All	All
Application	Spip	Spip	3.0.5	All	All	All
Application	Spip	Spip	3.0.6	All	All	All
Application	Spip	Spip	3.0.7	All	All	All
Application	Spip	Spip	3.0.8	All	All	All
Application	Spip	Spip	3.0.9	All	All	All
Application	Spip	Spip	2.0.1	All	All	All
Application	Spip	Spip	2.0.10	All	All	All
Application	Spip	Spip	2.0.11	All	All	All
Application	Spip	Spip	2.0.12	All	All	All
Application	Spip	Spip	2.0.13	All	All	All
Application	Spip	Spip	2.0.14	All	All	All

Application	Spip	Spip	2.0.15	All	All	All
Application	Spip	Spip	2.0.16	All	All	All
Application	Spip	Spip	2.0.17	All	All	All
Application	Spip	Spip	2.0.18	All	All	All
Application	Spip	Spip	2.0.19	All	All	All
Application	Spip	Spip	2.0.2	All	All	All
Application	Spip	Spip	2.0.20	All	All	All
Application	Spip	Spip	2.0.21	All	All	All
Application	Spip	Spip	2.0.22	All	All	All
Application	Spip	Spip	2.0.3	All	All	All
Application	Spip	Spip	2.0.4	All	All	All
Application	Spip	Spip	2.0.5	All	All	All
Application	Spip	Spip	2.0.6	All	All	All
Application	Spip	Spip	2.0.7	All	All	All
Application	Spip	Spip	2.0.8	All	All	All
Application	Spip	Spip	2.0.9	All	All	All
Application	Spip	Spip	2.1	All	All	All
Application	Spip	Spip	2.1.1	All	All	All
Application	Spip	Spip	2.1.10	All	All	All
Application	Spip	Spip	2.1.11	All	All	All
Application	Spip	Spip	2.1.12	All	All	All
Application	Spip	Spip	2.1.13	All	All	All
Application	Spip	Spip	2.1.14	All	All	All
Application	Spip	Spip	2.1.15	All	All	All
Application	Spip	Spip	2.1.16	All	All	All
Application	Spip	Spip	2.1.17	All	All	All
Application	Spip	Spip	2.1.18	All	All	All
Application	Spip	Spip	2.1.19	All	All	All
Application	Spip	Spip	2.1.2	All	All	All
Application	Spip	Spip	2.1.20	All	All	All
Application	Spip	Spip	2.1.21	All	All	All
Application	Spip	Spip	2.1.22	All	All	All
Application	Spip	Spip	2.1.23	All	All	All
Application	Spip	Spip	3.0.0	All	All	All
Application	Spip	Spip	3.0.1	All	All	All

Application	Spip	Spip	3.0.10	All	All	All
Application	Spip	Spip	3.0.11	All	All	All
Application	Spip	Spip	3.0.2	All	All	All
Application	Spip	Spip	3.0.3	All	All	All
Application	Spip	Spip	3.0.4	All	All	All
Application	Spip	Spip	3.0.5	All	All	All
Application	Spip	Spip	3.0.6	All	All	All
Application	Spip	Spip	3.0.7	All	All	All
Application	Spip	Spip	3.0.8	All	All	All
Application	Spip	Spip	3.0.9	All	All	All
Application	Spip	Spip	All	All	All	All
cpe:2.3:a:spip:spip:2.0.1:*****:						
cpe:2.3:a:spip:spip:2.0.10:*****:						
cpe:2.3:a:spip:spip:2.0.11:*****:						
cpe:2.3:a:spip:spip:2.0.12:*****:						
cpe:2.3:a:spip:spip:2.0.13:*****:						
cpe:2.3:a:spip:spip:2.0.14:*****:						
cpe:2.3:a:spip:spip:2.0.15:*****:						
cpe:2.3:a:spip:spip:2.0.16:*****:						
cpe:2.3:a:spip:spip:2.0.17:*****:						
cpe:2.3:a:spip:spip:2.0.18:*****:						
cpe:2.3:a:spip:spip:2.0.19:*****:						
cpe:2.3:a:spip:spip:2.0.2:*****:						
cpe:2.3:a:spip:spip:2.0.20:*****:						
cpe:2.3:a:spip:spip:2.0.21:*****:						
cpe:2.3:a:spip:spip:2.0.22:*****:						
cpe:2.3:a:spip:spip:2.0.3:*****:						
cpe:2.3:a:spip:spip:2.0.4:*****:						
cpe:2.3:a:spip:spip:2.0.5:*****:						
cpe:2.3:a:spip:spip:2.0.6:*****:						
cpe:2.3:a:spip:spip:2.0.7:*****:						

cpe:2.3:a:spip:spip:2.0.8:*****:
cpe:2.3:a:spip:spip:2.0.9:*****:
cpe:2.3:a:spip:spip:2.1:*****:
cpe:2.3:a:spip:spip:2.1.1:*****:
cpe:2.3:a:spip:spip:2.1.10:*****:
cpe:2.3:a:spip:spip:2.1.11:*****:
cpe:2.3:a:spip:spip:2.1.12:*****:
cpe:2.3:a:spip:spip:2.1.13:*****:
cpe:2.3:a:spip:spip:2.1.14:*****:
cpe:2.3:a:spip:spip:2.1.15:*****:
cpe:2.3:a:spip:spip:2.1.16:*****:
cpe:2.3:a:spip:spip:2.1.17:*****:
cpe:2.3:a:spip:spip:2.1.18:*****:
cpe:2.3:a:spip:spip:2.1.19:*****:
cpe:2.3:a:spip:spip:2.1.2:*****:
cpe:2.3:a:spip:spip:2.1.20:*****:
cpe:2.3:a:spip:spip:2.1.21:*****:
cpe:2.3:a:spip:spip:2.1.22:*****:
cpe:2.3:a:spip:spip:2.1.23:*****:
cpe:2.3:a:spip:spip:3.0.0:*****:
cpe:2.3:a:spip:spip:3.0.1:*****:
cpe:2.3:a:spip:spip:3.0.10:*****:
cpe:2.3:a:spip:spip:3.0.11:*****:
cpe:2.3:a:spip:spip:3.0.2:*****:
cpe:2.3:a:spip:spip:3.0.3:*****:
cpe:2.3:a:spip:spip:3.0.4:*****:
cpe:2.3:a:spip:spip:3.0.5:*****:
cpe:2.3:a:spip:spip:3.0.6:*****:

cpe:2.3:a:spip:spip:3.0.7:*****:
cpe:2.3:a:spip:spip:3.0.8:*****:
cpe:2.3:a:spip:spip:3.0.9:*****:
cpe:2.3:a:spip:spip:2.0.1:*****:
cpe:2.3:a:spip:spip:2.0.10:*****:
cpe:2.3:a:spip:spip:2.0.11:*****:
cpe:2.3:a:spip:spip:2.0.12:*****:
cpe:2.3:a:spip:spip:2.0.13:*****:
cpe:2.3:a:spip:spip:2.0.14:*****:
cpe:2.3:a:spip:spip:2.0.15:*****:
cpe:2.3:a:spip:spip:2.0.16:*****:
cpe:2.3:a:spip:spip:2.0.17:*****:
cpe:2.3:a:spip:spip:2.0.18:*****:
cpe:2.3:a:spip:spip:2.0.19:*****:
cpe:2.3:a:spip:spip:2.0.2:*****:
cpe:2.3:a:spip:spip:2.0.20:*****:
cpe:2.3:a:spip:spip:2.0.21:*****:
cpe:2.3:a:spip:spip:2.0.22:*****:
cpe:2.3:a:spip:spip:2.0.3:*****:
cpe:2.3:a:spip:spip:2.0.4:*****:
cpe:2.3:a:spip:spip:2.0.5:*****:
cpe:2.3:a:spip:spip:2.0.6:*****:
cpe:2.3:a:spip:spip:2.0.7:*****:
cpe:2.3:a:spip:spip:2.0.8:*****:
cpe:2.3:a:spip:spip:2.0.9:*****:
cpe:2.3:a:spip:spip:2.1:*****:
cpe:2.3:a:spip:spip:2.1.1:*****:
cpe:2.3:a:spip:spip:2.1.10:*****:
cpe:2.3:a:spip:spip:2.1.11:*****:

.
cpe:2.3:a:spip:spip:2.1.12:*****:
cpe:2.3:a:spip:spip:2.1.13:*****:
cpe:2.3:a:spip:spip:2.1.14:*****:
cpe:2.3:a:spip:spip:2.1.15:*****:
cpe:2.3:a:spip:spip:2.1.16:*****:
cpe:2.3:a:spip:spip:2.1.17:*****:
cpe:2.3:a:spip:spip:2.1.18:*****:
cpe:2.3:a:spip:spip:2.1.19:*****:
cpe:2.3:a:spip:spip:2.1.2:*****:
cpe:2.3:a:spip:spip:2.1.20:*****:
cpe:2.3:a:spip:spip:2.1.21:*****:
cpe:2.3:a:spip:spip:2.1.22:*****:
cpe:2.3:a:spip:spip:2.1.23:*****:
cpe:2.3:a:spip:spip:3.0.0:*****:
cpe:2.3:a:spip:spip:3.0.1:*****:
cpe:2.3:a:spip:spip:3.0.10:*****:
cpe:2.3:a:spip:spip:3.0.11:*****:
cpe:2.3:a:spip:spip:3.0.2:*****:
cpe:2.3:a:spip:spip:3.0.3:*****:
cpe:2.3:a:spip:spip:3.0.4:*****:
cpe:2.3:a:spip:spip:3.0.5:*****:
cpe:2.3:a:spip:spip:3.0.6:*****:
cpe:2.3:a:spip:spip:3.0.7:*****:
cpe:2.3:a:spip:spip:3.0.8:*****:
cpe:2.3:a:spip:spip:3.0.9:*****:
cpe:2.3:a:spip:spip:*****:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)