



CVE-2013-4555

Published on: 11/15/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:29 PM UTC

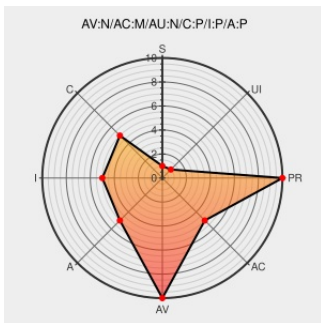
CVE-2013-4555

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Cross-site request forgery (CSRF) vulnerability in `ecrire/action/logout.php` in SPIP before 2.1.24 allows remote attackers to hijack the authentication of arbitrary users for requests that logout the user via unspecified vectors.

CVE-2013-4555 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

MEDIUM

Authentication

NONE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

PARTIAL

**Availability
Impact**

PARTIAL

CVE References

Description

Tags

Link

About Secunia Research | Flexera

[Vendor Advisory](#)
[secunia.com](#)
[Deprecated Link](#)
[text/plain](#)

[SECUNIA 55551](#)

Changements entre 2.1.23 et 2.1.24 - SPIP

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

[CONFIRM www.spip.net/fr_article5646.html](#)

Révision 20874 - Report de r20953 évitant le CSRF mais
* en évitant l'ajout de ask_php_auth d... - SPIP - SPIP
Core (Forge de développement)

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

[CONFIRM](#)
[core.spip.org/projects/spip/repository/revisions/20874](#)

SPIP Bugs Permit Cross-Site Request Forgery, Cross-
Site Scripting, and PHP Injections Attacks -
SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTRAK 1029317](#)

oss-security - Re: CVE Request: multiple vulnerabilities in spip

www.openwall.com

text/html

 MLIST [oss-security] 20131110 Re: CVE Request: multiple vulnerabilities in spip

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	2.0.0	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	2.1.1	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	2.1.3	All	All	All
Application	Spip	Spip	2.1.4	All	All	All
Application	Spip	Spip	2.1.5	All	All	All
Application	Spip	Spip	2.1.6	All	All	All
Application	Spip	Spip	2.1.7	All	All	All
Application	Spip	Spip	2.1.8	All	All	All
Application	Spip	Spip	2.1.9	All	All	All
Application	Spip	Spip	2.0.0	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	2.0.21	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	2.1.1	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	2.1.3	All	All	All
Application	Spip	Spip	2.1.4	All	All	All
Application	Spip	Spip	2.1.5	All	All	All
Application	Spip	Spip	2.1.6	All	All	All
Application	Spip	Spip	2.1.7	All	All	All
Application	Spip	Spip	2.1.8	All	All	All
Application	Spip	Spip	2.1.9	All	All	All
Application	Spip	Spip	All	All	All	All
cpe:2.3:a:spip:spip:2.0.0:*****:						
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:2.1.1:*****:
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:2.1.3:*****:
cpe:2.3:a:spip:spip:2.1.4:*****:
cpe:2.3:a:spip:spip:2.1.5:*****:
cpe:2.3:a:spip:spip:2.1.6:*****:
cpe:2.3:a:spip:spip:2.1.7:*****:
cpe:2.3:a:spip:spip:2.1.8:*****:
cpe:2.3:a:spip:spip:2.1.9:*****:
cpe:2.3:a:spip:spip:2.0.0:*****:
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:2.1.1:*****:
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:2.1.3:*****:
cpe:2.3:a:spip:spip:2.1.4:*****:
cpe:2.3:a:spip:spip:2.1.5:*****:
cpe:2.3:a:spip:spip:2.1.6:*****:
cpe:2.3:a:spip:spip:2.1.7:*****:

cpe:2.3:a:spip:spip:2.1.8:*****:
cpe:2.3:a:spip:spip:2.1.9:*****:
cpe:2.3:a:spip:spip:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→