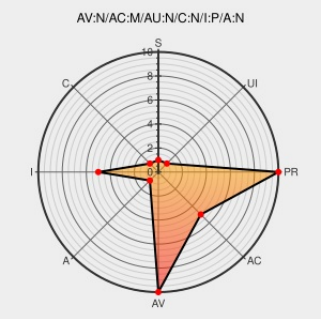
CVE-2013-4556

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

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

CVE-2013-4556

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Spip from Spip contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the author page (prive/formulaires/editer_auteur.php) in SPIP before 2.1.24 and 3.0.x before 3.0.12 allows remote attackers to inject arbitrary web script or HTML via the url_site parameter.

CVE-2013-4556 has been assigned by secalert@redhat.com 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
About Secunia Research | Flexera	Vendor Advisory, secunia.com, Depreciated 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 20879 - ne pas permettre n'importe quoi en url de site (report de r20876). - SPIP - SPIP Core (Forge de développement)	Patch, core.spip.org, text/html	CONFIRM core.spip.org/projects/spip/repository/revisions/20879
Révision 20880 - prive/formulaires/editer_auteur.php : ne pas permettre n'importe quoi en url ... - SPIP - SPIP Core	core.spip.org, text/html	CONFIRM core.spip.org/projects/spip/repository/revisions/20880

(Forge de développement)		
SPIP Bugs Permit Cross-Site Request Forgery, Cross-Site Scripting, and PHP Injections Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1029317
Debian -- Security Information -- DSA-2794-1 spip	www.debian.org Depreciated Link text/html	DEBIAN DSA-2794
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

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	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	2.0.0	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	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:2.0.0:*:*:*:*:*:*:*:

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: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:2.0.0:*:*:*:*:*:*:*:

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:2.0.17:*:*:*:*:*:*:*:

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: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

← Previous ID

Next ID→