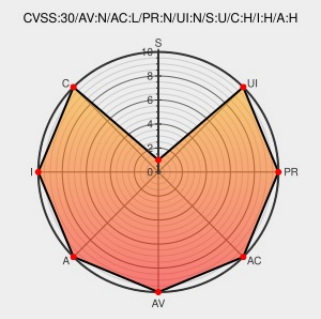
CVE-2017-9736

Published on: 06/17/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:57 PM UTC

CVE-2017-9736

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



Certain versions of Spip from Spip contain the following vulnerability:

SPIP 3.1.x before 3.1.6 and 3.2.x before Beta 3 does not remove shell metacharacters from the host field, allowing a remote attacker to cause remote code execution.

CVE-2017-9736 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3890-1 spip	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3890
Révision 23593 - Report de r23590 : Utiliser des simples quotes	Patch	CONFIRM

dans la fonction anonyme, c'es... - SPIP - SPIP Core (Forge de développement)	Vendor Advisory core.spip.net text/html	core.spip.net/projects/spip/repository/revisions/23593
Révision 23594 - Report de r23591 : Meilleure sanitization du host pour eviter des choses exot... - SPIP - SPIP Core (Forge de développement)	Patch Vendor Advisory core.spip.net text/html	CONFIRM core.spip.net/projects/spip/repository/revisions/23594
CRITICAL security update : SPIP 3.1.6 and SPIP 3.2 Beta 3 - SPIP-Contrib	Vendor Advisory contrib.spip.net text/html	CONFIRM contrib.spip.net/CRITICAL-security-update-SPIP-3-1-6-and-SPIP-3-2-Beta

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	3.1.0	All	All	All
Application	Spip	Spip	3.1.0	alpha	All	All
Application	Spip	Spip	3.1.0	beta	All	All
Application	Spip	Spip	3.1.0	rc	All	All
Application	Spip	Spip	3.1.0	rc2	All	All
Application	Spip	Spip	3.1.0	rc3	All	All
Application	Spip	Spip	3.1.1	All	All	All
Application	Spip	Spip	3.1.2	All	All	All
Application	Spip	Spip	3.1.3	All	All	All
Application	Spip	Spip	3.1.4	All	All	All
Application	Spip	Spip	3.1.5	All	All	All
Application	Spip	Spip	3.2	alpha-1	All	All
Application	Spip	Spip	3.2.0	beta	All	All
Application	Spip	Spip	3.2.0	beta2	All	All
Application	Spip	Spip	3.1.0	All	All	All
Application	Spip	Spip	3.1.0	alpha	All	All
Application	Spip	Spip	3.1.0	beta	All	All
Application	Spip	Spip	3.1.0	rc	All	All
Application	Spip	Spip	3.1.0	rc2	All	All
Application	Spip	Spip	3.1.0	rc3	All	All
Application	Spip	Spip	3.1.1	All	All	All

Application	Spip	Spip	3.1.2	All	All	All
Application	Spip	Spip	3.1.3	All	All	All
Application	Spip	Spip	3.1.4	All	All	All
Application	Spip	Spip	3.1.5	All	All	All
Application	Spip	Spip	3.2	alpha-1	All	All
Application	Spip	Spip	3.2.0	beta	All	All
Application	Spip	Spip	3.2.0	beta2	All	All

cpe:2.3:a:spip:spip:3.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:alpha:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:beta:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:rc:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.2:alpha-1:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.2.0:beta:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.2.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:alpha:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:beta:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:rc:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.2:alpha-1:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.2.0:beta:*:*:*:*:*:*:

cpe:2.3:a:spip:spip:3.2.0:beta2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© 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 registred 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