



CVE-2016-9997

Published on: 12/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9997

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

SPIP 3.1.x suffers from a Reflected Cross Site Scripting Vulnerability in `/ecrire/exec/puce_statut.php` involving the ``$id`` parameter, as demonstrated by a `/ecrire/?exec=puce_statut` URL.

CVE-2016-9997 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

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
SPiP Input Validation Flaws in 'id' and 'plugin' Parameters Let Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRAK 1037486
Révision 23288 - Fix #3845 : sécuriser les exec	Issue Tracking	CONFIRM

 BID 95008

There are currently no QIDs associated with this CVE

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	3.1.0	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
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:3.1.0:*****:
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:*****:

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 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](#)