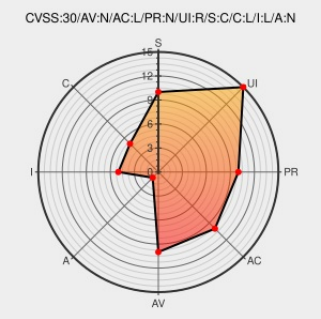
# CVE-2016-9998

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

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

## CVE-2016-9998

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




Certain versions of Spip from Spip contain the following vulnerability:

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

CVE-2016-9998 has been assigned by 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 | SECTRACK 1037486 |
| Révision 23288 - Fix #3845 : sécuriser les exec | Issue Tracking | CONFIRM |

| | | |
|---|---|---|
| info_plugin et puce_statut merci à felixk3y d... - SPIP - SPIP Core (Forge de développement) | Patch<br>Vendor Advisory<br>core.spip.net<br>text/html | core.spip.net/projects/spip/repository/revisions/23288 |
| SPIP Multiple Cross Site Scripting Vulnerabilities | Third Party Advisory<br>VDB Entry<br>cve.report (archive)<br>text/html | BID 95008 |



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 | 3.1.0 | 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→