



CVE-2016-7982

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-7982
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-18 17:59:00 UTC
Updated	2017-05-24 01:29:00 UTC
Description	Directory traversal vulnerability in ecrire/exec/valider_xml.php in SPIP 3.1.2 and earlier allows remote attackers to enumera

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spip	Spip	All	All	All	All

References

Reference
oss-security - Re: SPIP vulnerabilities: request for 5 CVE
SPIP Multiple Security Vulnerabilities
oss-security - CVE-2016-7982: SPIP 3.1.1/3.1.2 File Enumeration / Path Traversal
oss-security - SPIP vulnerabilities: request for 5 CVE
Révision 23200 - - ?exec=valider_xml n'est executable que par les webmestres - var_url ne doit... - SPIP - SPIP Core (Forge de développeme
Sysdream, SPIP 3.1.1/3.1.2 File Enumeration / Path Traversal (CVE-2016-7982)
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)