



CVE-2006-0976

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

Summary

CVE	CVE-2006-0976
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-03 11:02:00 UTC
Updated	2018-10-18 16:30:00 UTC
Description	Directory traversal vulnerability in scan_lang_insert.php in Boris Herbinier-Seve SPiD 1.3.1 allows remote attackers to read arbitrary files.

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spid	Spid	1.3.1	All	All	All
Application	Spid	Spid	1.3.1	All	All	All

References

Reference

SecurityFocus

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SPiD Scan_Lang_Insert.PHP Local File Include Vulnerability

IBM X-Force Exchange

nsag.ru - This website is for sale! - nsag saga nsagc usagi sage snagit snag a job nsa gov usagx sagd ncegifts com Resources an

SPiD scan_lang_insert.php File Inclusion Vulnerability - Advisories - Secunia

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](#)