



CVE-2014-3129

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

Summary

CVE	CVE-2014-3129
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-30 14:22:00 UTC
Updated	2014-05-10 04:06:00 UTC
Description	The Java Server Pages in the Software Lifecycle Manager (SLM) in SAP NetWeaver allows remote attackers to obtain sensitive information.

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Software Lifecycle Manager	7.1	All	All	All
Application	Sap	Netweaver Software Lifecycle Manager	7.1	All	All	All

References

Reference	Source	Link
Page Not Found Onapsis	MISC	w
Acknowledgments to Security Researchers SCN	CONFIRM	sc
service.sap.com/sap/support/notes/1894049	CONFIRM	se
Full Disclosure: [Onapsis Security Advisory 2014-005] Information disclosure in SAP Software Lifecycle Manager	FULLDISC	se
SAP Software Lifecycle Manager JSP Pages Let Remote Users Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	w
SAP Solution Manager Remote Information Disclosure Vulnerability	BID	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

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](#)