



CVE-2014-4003

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

Summary

CVE	CVE-2014-4003
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-09 20:55:00 UTC
Updated	2018-10-09 19:47:00 UTC
Description	The System Landscape Directory (SLD) in SAP NetWeaver allows remote attackers to modify information via vectors relate

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver	-	All	All	All
Application	Sap	Netweaver	-	All	All	All

References

Reference	Source
Acknowledgments to Security Researchers SCN	CONFIRM
SecurityFocus	BUGTRAC
SAP System Landscape Directory Unauthorized Access Vulnerability	BID
Full Disclosure: [Onapsis Security Advisory 2014-020] SAP SLD Information Tampering	FULLDISC
service.sap.com/sap/support/notes/1939334	CONFIRM
SAP SLD Information Tampering ≈ Packet Storm	MISC
Security Advisory SA58633 - SAP NetWeaver System Landscape Directory Component Security Bypass Vulnerability - Secunia	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)