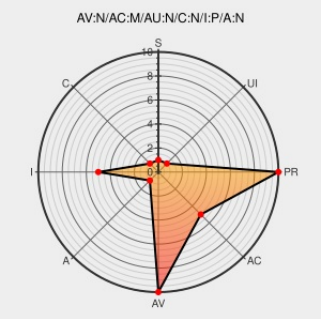
CVE-2010-2904

Published on: 07/28/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

CVE-2010-2904

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



Certain versions of Netweaver from Sap contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the System Landscape Directory (SLD) component 6.4 through 7.02 in SAP NetWeaver allow remote attackers to inject arbitrary web script or HTML via the (1) action parameter to testsdic and the (2) helpstring parameter to paramhelp.jsp.

CVE-2010-2904 has been assigned by cve@mitre.org to track the vulnerability

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
Files ≈ Packet Storm	packetstormsecurity.org text/plain	MISC packetstormsecurity.org/1007-advisories/DSECRG-09-068.txt
SAP NetWeaver System Landscape Directory Component Cross-Site Scripting - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 40712
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2010-1935
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF sapnetweaver-paramhelp-xss(60668)
No Description Provided	www.osvdb.org	OSVDB 66640

	Inactive Link Not Archived	
Digital Security Research Group - [DSECRG-09-068] SAP NetWaver SLD - Multiple XSS	web.archive.org text/html Inactive Link Not Archived	MISC dsecrg.com/pages/vul/show.php?id=168
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 66639
No Description Provided	service.sap.com text/html	MISC service.sap.com/sap/support/notes/1416047

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver	All	All	All	All
Application	Sap	Netweaver	6.4	All	All	All
Application	Sap	Netweaver	7.0	All	All	All
Application	Sap	Netweaver	All	All	All	All
Application	Sap	Netweaver	6.4	All	All	All
Application	Sap	Netweaver	7.0	All	All	All
Application	Sap	System Landscape Directory	6.4	All	All	All
Application	Sap	System Landscape Directory	7.0	All	All	All
Application	Sap	System Landscape Directory	7.02	All	All	All
Application	Sap	System Landscape Directory	6.4	All	All	All
Application	Sap	System Landscape Directory	7.0	All	All	All
Application	Sap	System Landscape Directory	7.02	All	All	All

cpe:2.3:a:sap:netweaver:*:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:6.4:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:*:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:6.4:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:sap:system_landscape_directory:6.4:*:*:*:*:*:*:*:

cpe:2.3:a:sap:system_landscape_directory:7.0:*:*:*:*:*:*:*

cpe:2.3:a:sap:system_landscape_directory:7.02:*:*:*:*:*:*:*

cpe:2.3:a:sap:system_landscape_directory:6.4:*:*:*:*:*:*:*

cpe:2.3:a:sap:system_landscape_directory:7.0:*:*:*:*:*:*:*

cpe:2.3:a:sap:system_landscape_directory:7.02:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→