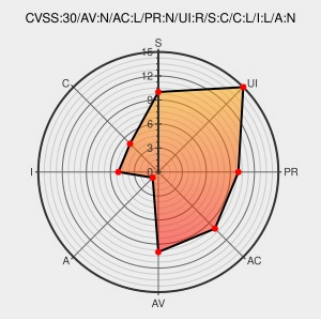
CVE-2016-2387

Published on: 02/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:15 PM UTC

CVE-2016-2387

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 Java Proxy Runtime ProxyServer servlet in SAP NetWeaver 7.4 allow remote attackers to inject arbitrary web script or HTML via the (1) ns or (2) interface parameter to ProxyServer/register, aka SAP Security Note 2220571.

CVE-2016-2387 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

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
[ERPSCAN-16-008] SAP NetWeaver 7.4 (ProxyServer servlet) - XSS vulnerability	erpscan.io text/html	MISC erpscan.io/advisories/erpscan-16-008-sap-netweaver-7-4-proxyserver-servlet-xss-vulnerability/
SAP Security Notes February 2016 - Manufacturing	erpscan.io	MISC erpscan.io/press-center/blog/sap-security-

SAP Security Notes February 2016 - Manufacturing Cybersecurity	text/html	notes-february-2016-review/
SAP NetWeaver AS JAVA 7.4 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/137045/SAP-NetWeaver-AS-JAVA-7.4-Cross-Site-Scripting.html
Full Disclosure: [ERPSCAN-16-008] SAP NetWeaver AS JAVA - XSS vulnerability in ProxyServer servlet	seclists.org text/html	FULLDISC 20160517 [ERPSCAN-16-008] SAP NetWeaver AS JAVA - XSS vulnerability in ProxyServer servlet

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	7.40	All	All	All
Application	Sap	Netweaver	7.40	All	All	All

cpe:2.3:a:sap:netweaver:7.40:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:7.40:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→