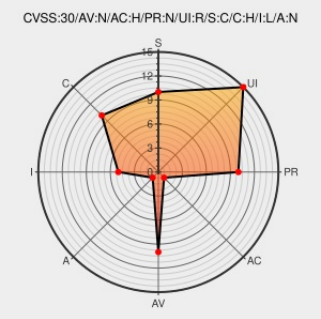
# CVE-2021-33691

Published on: 09/15/2021 12:00:00 AM UTC

Last Modified on: 09/28/2021 03:05:00 PM UTC

## CVE-2021-33691

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




Certain versions of Netweaver Development Infrastructure from Sap contain the following vulnerability:

NWDI Notification Service versions - 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.SAP NetWeaver Development Infrastructure Notification Service allows a threat actor to send crafted scripts to a victim. If the victim has an active session when the crafted script gets executed, the threat actor could compromise information in victims session, and gain access to some sensitive information also.

CVE-2021-33691 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Development Infrastructure (Notification Service)** version **7.31**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Development Infrastructure (Notification Service)** version **7.40**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver Development Infrastructure (Notification Service)** version **7.50**

### 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 |
|---|---|---|
| No Description Provided | launchpad.support.sap.com<br>text/html | MISC<br>launchpad.support.sap.com/#/notes/3073450 |
| SAP Security Patch Day – August 2021 - Product Security Response at SAP - Community Wiki | wiki.scn.sap.com<br>text/html | MISC<br>wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=582222806 |

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 Development Infrastructure | 7.31 | All | All | All |
| Application | Sap | Netweaver Development Infrastructure | 7.40 | All | All | All |
| Application | Sap | Netweaver Development Infrastructure | 7.50 | All | All | All |

cpe:2.3:a:sap:netweaver_development_infrastructure:7.31:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_development_infrastructure:7.40:*:*:*:*:*:*:*

cpe:2.3:a:sap:netweaver_development_infrastructure:7.50:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2021-33691 : NWDI Notification Service versions - 7.31, 7.40, 7.50, does not sufficiently encode user-controlle… twitter.com/i/web/status/1… | 2021-09-15 18:43:21 |

← Previous ID  Next ID→

© CVE.report 2023 | |
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 registred 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.

**CVE.report and Source URL Uptime Status** status.cve.report