



# CVE-2019-0282

Published on: 04/10/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:03 PM UTC

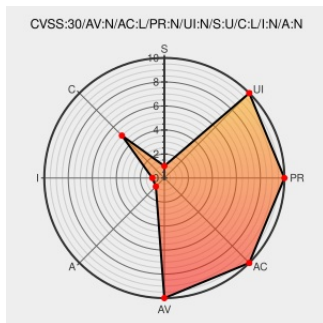
## CVE-2019-0282

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Netweaver Process Integration](#) from [Sap](#) contain the following vulnerability:

Several web pages in SAP NetWeaver Process Integration (Runtime Workbench), fixed in versions 7.10 to 7.11, 7.30, 7.31, 7.40, 7.50; can be accessed without user authentication, which might expose internal data like release information, Java package and Java object names which can be misused by the attacker.

CVE-2019-0282 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Process Integration (Runtime Workbench)** version **from 7.10 to 7.11**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Process Integration (Runtime Workbench)** version **7.30**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Process Integration (Runtime Workbench)** version **7.31**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Process Integration (Runtime Workbench)** version **7.40**

Affected Vendor/Software: [SAP](#) **SAP SE - SAP NetWeaver Process Integration (Runtime Workbench)** version **7.50**

CVSS3 Score: **5.3 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |

| impact  | impact | impact |
|---------|--------|--------|
| PARTIAL | NONE   | NONE   |

## CVE References

| Description                                                                             | Tags                                                                                                                 | Link                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SAP Security Patch Day – April 2019 - Product Security Response at SAP - Community Wiki | <div>Vendor Advisory</div> <div>wiki.scn.sap.com</div> <div>text/html</div>                                          | <div> CONFIRM</div> <div>wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=517899114</div> |
| No Description Provided                                                                 | <div>Permissions Required</div> <div>Vendor Advisory</div> <div>launchpad.support.sap.com</div> <div>text/html</div> | <div> CONFIRM</div> <div>launchpad.support.sap.com/#/notes/2742758</div>                     |

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](mailto: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 Process Integration | 7.10    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.11    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.30    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.31    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.40    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.50    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.10    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.11    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.30    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.31    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.40    | All    | All     | All      |
| Application                                               | Sap    | Netweaver Process Integration | 7.50    | All    | All     | All      |
| cpe:2.3:a:sap:netweaver_process_integration:7.10:*****:.* |        |                               |         |        |         |          |
| cpe:2.3:a:sap:netweaver_process_integration:7.11:*****:.* |        |                               |         |        |         |          |
| cpe:2.3:a:sap:netweaver_process_integration:7.30:*****:.* |        |                               |         |        |         |          |
| cpe:2.3:a:sap:netweaver_process_integration:7.31:*****:.* |        |                               |         |        |         |          |
| cpe:2.3:a:sap:netweaver_process_integration:7.40:*****:.* |        |                               |         |        |         |          |
|                                                           |        |                               |         |        |         |          |
|                                                           |        |                               |         |        |         |          |

|                                                             |
|-------------------------------------------------------------|
| cpe:2.3:a:sap:netweaver_process_integration:7.50:*:*:*:*:*: |
| cpe:2.3:a:sap:netweaver_process_integration:7.10:*:*:*:*:*: |
| cpe:2.3:a:sap:netweaver_process_integration:7.11:*:*:*:*:*: |
| cpe:2.3:a:sap:netweaver_process_integration:7.30:*:*:*:*:*: |
| cpe:2.3:a:sap:netweaver_process_integration:7.31:*:*:*:*:*: |
| cpe:2.3:a:sap:netweaver_process_integration:7.40:*:*:*:*:*: |
| cpe:2.3:a:sap:netweaver_process_integration:7.50:*:*:*:*:*: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)