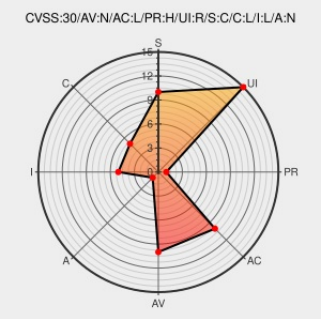
CVE-2019-0316

Published on: 06/14/2019 12:00:00 AM UTC

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

CVE-2019-0316

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



Certain versions of Netweaver Process Integration from Sap contain the following vulnerability:

SAP NetWeaver Process Integration, versions: SAP_XIESR: 7.20, SAP_XITOOL: 7.10 to 7.11, 7.30, 7.31, 7.40, 7.50, does not sufficiently validate user-controlled inputs, which allows an attacker possessing admin privileges to read and modify data from the victim's browser, by injecting malicious scripts in certain servlets, which will be executed when the victim is tricked to click on those malicious links, resulting in reflected Cross Site Scripting vulnerability.

CVE-2019-0316 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
SAP Security Patch Day – June 2019 – Product Security	Vendor Advisory	MISC

SAP Security Patch Day – June 2019 - Product Security Response at SAP - Community Wiki	Vendor Advisory wiki.scn.sap.com text/html	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=521864242
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2745917

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	7.20	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	7.20	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:7.20:*:*:*:*:*:*:*:

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:7.20:*:*:*:*:*:*:*

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→