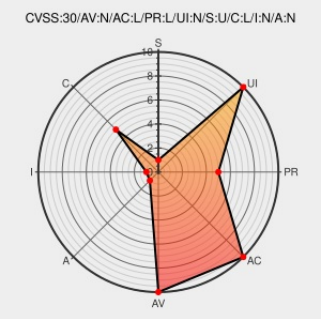
CVE-2020-6371

Published on: 10/14/2020 12:00:00 AM UTC

Last Modified on: 10/05/2022 02:16:00 PM UTC

CVE-2020-6371

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



Certain versions of Netweaver Application Server Abap from Sap contain the following vulnerability:

User enumeration vulnerability can be exploited to get a list of user accounts and personal user information can be exposed in SAP NetWeaver Application Server ABAP (POWL test application) versions - 710, 711, 730, 731, 740, 750, leading to Information Disclosure.

CVE-2020-6371 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2963137

SAP Security Patch Day – October 2020 - 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=558632196

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 Application Server Abap	710	All	All	All
Application	Sap	Netweaver Application Server Abap	711	All	All	All
Application	Sap	Netweaver Application Server Abap	730	All	All	All
Application	Sap	Netweaver Application Server Abap	731	All	All	All
Application	Sap	Netweaver Application Server Abap	740	All	All	All
Application	Sap	Netweaver Application Server Abap	750	All	All	All
Application	Sap	Netweaver As Abap	710	All	All	All
Application	Sap	Netweaver As Abap	711	All	All	All
Application	Sap	Netweaver As Abap	730	All	All	All
Application	Sap	Netweaver As Abap	731	All	All	All
Application	Sap	Netweaver As Abap	740	All	All	All
Application	Sap	Netweaver As Abap	750	All	All	All
Application	Sap	Netweaver As Abap	710	All	All	All
Application	Sap	Netweaver As Abap	711	All	All	All
Application	Sap	Netweaver As Abap	730	All	All	All
Application	Sap	Netweaver As Abap	731	All	All	All
Application	Sap	Netweaver As Abap	740	All	All	All
Application	Sap	Netweaver As Abap	750	All	All	All

cpe:2.3:a:sap:netweaver_application_server_abap:710:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:711:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:730:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:731:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:740:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_application_server_abap:750:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:710:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:711:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:730:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:731:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:740:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:750:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:710:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:711:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:730:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:731:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:740:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_abap:750:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | User enumeration vulnerability can be ex... | CVE-2020-6371 | Link for more: alerts.remotelyrmm.com/CVE-2020-6371	2022-10-05 15:32:16

← Previous ID

Next ID→