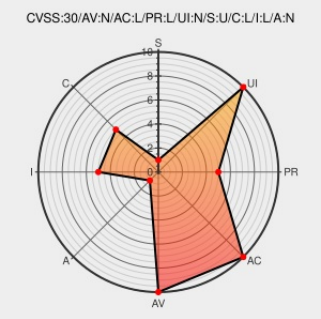
CVE-2020-6178

Published on: 03/10/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-6178

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



Certain versions of Enable Now from Sap contain the following vulnerability:

SAP Enable Now, before version 1911, sends the Session ID cookie value in URL. This might be stolen from the browser history or log files, leading to Information Disclosure.

CVE-2020-6178 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP Enable Now** version **before version 1911**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	Permissions Required launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2880664

SAP Security Patch Day – March 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=540935305

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Enable Now	All	All	All	All
Application	Sap	Enable Now	All	All	All	All

cpe:2.3:a:sap:enable_now:*:*:*:*:*:*:*:*:

cpe:2.3:a:sap:enable_now:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→