CVE-2021-27608

Published on: 04/14/2021 12:00:00 AM UTC

Last Modified on: 04/20/2021 09:45:00 PM UTC

CVE-2021-27608

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

Certain versions of Setup from Sap contain the following vulnerability:

An unquoted service path in SAPSetup, version - 9.0, could lead to privilege escalation during the installation process that is performed when an executable file is registered. This could further lead to complete compromise of confidentiality, Integrity and Availability.

CVE-2021-27608 has been assigned by cna@sap.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SAP SE** - **SAP Setup** version **9.0**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 4.4 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/3039649

SAP Security Patch Day – April 2021 - Product Security Response at SAP - Community Wiki	wiki.scn.sap.com text/html	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Setup	9.0	All	All	All

cpe:2.3:a:sap:setup:9.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-27608 : An unquoted service path in #SAPSetup, version - 9.0, could lead to privilege escalation during th… twitter.com/i/web/status/1…	2021-04-14 15:04:26
/r/netcve	CVE-2021-27608	2021-04-14 15:46:40

← Previous ID

Next ID→