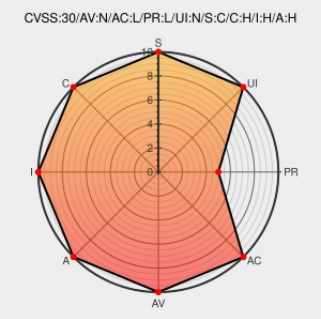
CVE-2021-38163

Published on: 09/14/2021 12:00:00 AM UTC

Last Modified on: 09/24/2021 03:52:00 PM UTC

CVE-2021-38163

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Netweaver from Sap contain the following vulnerability:

SAP NetWeaver (Visual Composer 7.0 RT) versions - 7.30, 7.31, 7.40, 7.50, without restriction, an attacker authenticated as a non-administrative user can upload a malicious file over a network and trigger its processing, which is capable of running operating system commands with the privilege of the Java Server process. These commands can be used to read or modify any information on the server or shut the server down making it unavailable.

CVE-2021-38163 has been assigned by cna@sap.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Visual Composer 7.0 RT)** version **7.30**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Visual Composer 7.0 RT)** version **7.31**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Visual Composer 7.0 RT)** version **7.40**

Affected Vendor/Software: **SAP SE** - **SAP NetWeaver (Visual Composer 7.0 RT)** version **7.50**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
No Description Provided	launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/3084487
SAP Security Patch Day – September 2021 - Product Security Response at SAP - Community Wiki	wiki.scn.sap.com text/html	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=585106405

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	7.30	All	All	All
Application	Sap	Netweaver	7.31	All	All	All
Application	Sap	Netweaver	7.40	All	All	All
Application	Sap	Netweaver	7.50	All	All	All

cpe:2.3:a:sap:netweaver:7.30:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:7.31:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:7.40:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:7.50:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-38163 : #SAP NetWeaver Visual Composer 7.0 RT versions - 7.30, 7.31, 7.40, 7.50, without restriction, an… twitter.com/i/web/status/1…	2021-09-14 12:11:03
@ThreatMonIT	• [CVE-2021-38163] Unrestricted File Upload vulnerability in SAP NetWeaver (Visual Composer 7.0 RT) • [CVE-2021-375… twitter.com/i/web/status/1…	2021-09-14 19:33:33
@ptswarm	⚡SAP fixed Post-Auth RCE (CVE-2021-38163) in SAP NetWeaver found by our researcher Mikhail Klyuchnikov. CVSS 9.9… twitter.com/i/web/status/1…	2021-09-15 14:14:06
@autumn_good_35	CVE-2021-38163 twitter.com/ptswarm/status…	2021-09-15 14:45:29

@GrupoICA_Ciber	?SAP? Múltiples vulnerabilidades de severidad alta en productos SAP: CVE-2021-33672,CVE-2021-38162,CVE-2021-38163… twitter.com/i/web/status/1…	2021-09-25 08:23:14

← Previous ID

Next ID→