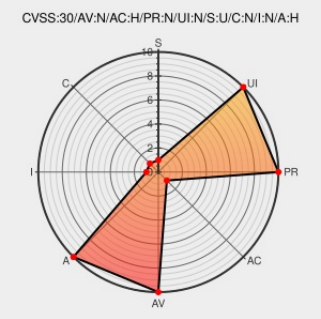
CVE-2021-27624

Published on: 06/09/2021 12:00:00 AM UTC

Last Modified on: 10/31/2022 02:47:00 PM UTC

CVE-2021-27624

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



Certain versions of Netweaver As Internet Graphics Server from Sap contain the following vulnerability:

SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieving an existing system state value can submit a malicious IGS request over a network which due to insufficient input validation in method CiXMLIStreamRawBuffer::readRaw () which will trigger an internal memory corruption error in the system causing the system to crash and rendering it unavailable. In this attack, no data in the system can be viewed or modified.

CVE-2021-27624 has been assigned by cna@sap.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SAP SE** - **SAP Internet Graphics Service** version **7.20**

Affected Vendor/Software: **SAP SE** - **SAP Internet Graphics Service** version **7.20EXT**

Affected Vendor/Software: **SAP SE** - **SAP Internet Graphics Service** version **7.53**

Affected Vendor/Software: **SAP SE** - **SAP Internet Graphics Service** version **7.20_EX2**

Affected Vendor/Software: **SAP SE** - **SAP Internet Graphics Service** version **7.81**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: Onapsis Security Advisory 2021-0019: [Multiple CVEs] Memory Corruption vulnerability in SAP NetWeaver ABAP IGS service	seclists.org text/html	FULLDISC 20211022 Onapsis Security Advisory 2021-0019: [Multiple CVEs] Memory Corruption vulnerability in SAP NetWeaver ABAP IGS service
No Description Provided	launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/3021050
SAP Security Patch Day – June 2021 - Product Security Response at SAP - Community Wiki	wiki.scn.sap.com text/html	MISC wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999
SAP NetWeaver ABAP IGS Memory Corruption ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/164598/SAP-NetWeaver-ABAP-IGS-Memory-Corruption.html

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 As Internet Graphics Server	7.20	All	All	All
Application	Sap	Netweaver As Internet Graphics Server	7.20ex2	All	All	All
Application	Sap	Netweaver As Internet Graphics Server	7.20ext	All	All	All
Application	Sap	Netweaver As Internet Graphics Server	7.53	All	All	All
Application	Sap	Netweaver As Internet Graphics Server	7.81	All	All	All

cpe:2.3:a:sap:netweaver_as_internet_graphics_server:7.20:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_internet_graphics_server:7.20ex2:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_internet_graphics_server:7.20ext:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_internet_graphics_server:7.53:*:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver_as_internet_graphics_server:7.81:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-27624 : #SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthentica… twitter.com/i/web/status/1…	2021-06-09 14:05:58

← Previous ID

Next ID→