



# CVE-2021-27623

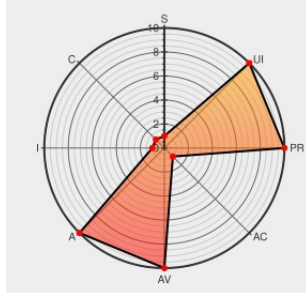
Published on: 06/09/2021 12:00:00 AM UTC

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

## CVE-2021-27623

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



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 CXmlUtility::CheckLength() 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-2021-27623 has been assigned by [SAP](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Service** version 7.20

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Service** version 7.20EXT

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Service** version 7.53

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Service** version 7.20\_EX2

Affected Vendor/Software: [SAP](#) **SAP SE - SAP Internet Graphics Service** version 7.81

CVSS3 Score: **5.9 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

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                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No Description Provided                                                                | <a href="https://launchpad.support.sap.com">launchpad.support.sap.com</a><br><a href="#">text/html</a> |  MISC<br><a href="https://launchpad.support.sap.com/#/notes/3021050">launchpad.support.sap.com/#/notes/3021050</a>                                       |
| SAP Security Patch Day – June 2021 - Product Security Response at SAP - Community Wiki | <a href="https://wiki.scn.sap.com">wiki.scn.sap.com</a><br><a href="#">text/html</a>                   |  MISC<br><a href="https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999">wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

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-2021-27623 : #SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthentica... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-06-09 14:05:40 |

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)