



CVE-2021-27622

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-27622
State	PUBLIC
Assigner	cna@sap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-09 14:15:00 UTC
Updated	2022-10-31 14:47:00 UTC
Description	SAP Internet Graphics Service, versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81, allows an unauthenticated attacker after retrieval of a valid session ID to perform a Denial of Service (DoS) attack by sending a large number of requests to the service.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Full Disclosure: Onapsis Security Advisory 2021-0019: [Multiple CVEs] Memory Corruption vulnerability in SAP NetWeaver ABAP IGS service
launchpad.support.sap.com
SAP Security Patch Day – June 2021 - Product Security Response at SAP - Community Wiki
SAP NetWeaver ABAP IGS Memory Corruption ≈ Packet Storm
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)