



CVE-2021-29672

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

Summary

CVE	CVE-2021-29672
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-26 17:15:00 UTC
Updated	2022-09-30 15:18:00 UTC
Description	IBM Spectrum Protect Client 8.1.0.0-8 through 1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bc

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Spectrum Protect Client	All	All	All	All
Application	ibm	Spectrum Protect For Space Management	All	All	All	All

References

Reference
IBM X-Force Exchange
IBM Spectrum Protect: Multiple Vulnerabilities (GLSA 202209-02) — Gentoo security
Security Bulletin: Stack-based Buffer Overflow vulnerabilities in IBM Spectrum Protect Back-up Archive Client and IBM Spectrum Protect for S
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710616 Gentoo Linux IBM Spectrum Protect Multiple Vulnerabilities (GLSA 202209-02)

© [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](#)