



CVE-2023-35897

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

Summary

CVE	CVE-2023-35897
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-06 14:15:00 UTC
Updated	2023-10-11 17:21:00 UTC
Description	IBM Spectrum Protect Client and IBM Storage Protect for Virtual Environments 8.1.0.0 through 8.1.19.0 could allow a local

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Storage Protect	All	All	All	All
Application	ibm	Storage Protect	All	All	All	All
Application	ibm	Storage Protect Client	All	All	All	All

References

Reference

- Security Bulletin: IBM Storage Protect Backup-Archive Client and IBM Storage Protect for Virtual Environments are vulnerable to arbitrary code execution
- IBM X-Force Exchange
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378897 IBM Storage Protect Backup-Archive Client Arbitrary Code Execution (ACE) Vulnerability (7037299)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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