Security Bulletin:IBM Storage Protect Server is affected by a vulnerability that could allow authenticated users to access administrative metadata through the JSON-RPC endpoint (CVE-2025-13855).

Security Bulletin

Summary

IBM Storage Protect Server provides a JSON-RPC endpoint through which authenticated users can execute backend SQL SELECT queries and access data from internal database tables, potentially exposing administrative metadata.

Vulnerability Details

CVEID: CVE-2025-13855 *(https://www.cve.org/CVERecord?id=CVE-2025-13855)*

DESCRIPTION: IBM Storage Protect Plus Server is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.

CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(https://cwe.mitre.org/data/definitions/89.html)*

CVSS Source: IBM

CVSS Base score: 7.6

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Storage Protect Server	8.2.0

None

Get Notified about Future Security Bulletins

Subscribe to My Notifications *(https://www.ibm.com/support/pages/node/718119)* to be notified of important product support alerts like this.

References

Complete CVSS v3 Guide

On-line Calculator v3

Related Information

IBM Secure Engineering Web Portal *(http://www.ibm.com/security/secure-engineering/bulletins.html)*

IBM Product Security Incident Response Blog *(http://www.ibm.com/blogs/psirt)*

Acknowledgement

This vulnerability was reported to IBM by Umar Butt (umar.butt@protiviti.de), Ayman Madhour (ayman.madhour@protiviti.de), and Saed Alavi (Saed.Alavi@protiviti.de).

Change History

26 Mar 2026: Initial Publication

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are

unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Document Information

More support for:

IBM Spectrum Protect *(https://www.ibm.com/mysupport/s/topic/0TO50000000IQWvGAO)*

Software version:

8.2

Operating system(s):

AIX, Linux, Windows

Document number:

7267783

Modified date:

03 April 2026

Initial Publish date:

26 March 2026