



CVE-2018-1438

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2018-1438 |
| State | PUBLIC |
| Assigner | psirt@us.ibm.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-05-17 21:29:00 UTC |
| Updated | 2020-08-19 19:11:00 UTC |
| Description | IBM SAN Volume Controller, IBM Storwize, IBM Spectrum Virtualize and IBM FlashSystem products (6.1, 6.2, 6.3, 6.4, 7.1 |

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|--------------------------------------|---------|--------|---------|----------|
| Hardware | ibm | San Volume Controller | - | All | All | All |
| Hardware | ibm | San Volume Controller | - | All | All | All |
| Operating System | ibm | San Volume Controller Firmware | All | All | All | All |
| Operating System | ibm | San Volume Controller Firmware | All | All | All | All |
| Application | ibm | Spectrum Virtualize | All | All | All | All |
| Application | ibm | Spectrum Virtualize | All | All | All | All |
| Application | ibm | Spectrum Virtualize For Public Cloud | All | All | All | All |
| Application | ibm | Spectrum Virtualize For Public Cloud | All | All | All | All |
| Hardware | ibm | Storwize V3500 | - | All | All | All |
| Hardware | ibm | Storwize V3500 | - | All | All | All |
| Operating System | ibm | Storwize V3500 Firmware | All | All | All | All |
| Operating System | ibm | Storwize V3500 Firmware | All | All | All | All |
| Hardware | ibm | Storwize V3700 | - | All | All | All |
| Hardware | ibm | Storwize V3700 | - | All | All | All |
| Operating System | ibm | Storwize V3700 Firmware | All | All | All | All |
| Operating System | ibm | Storwize V3700 Firmware | All | All | All | All |
| Hardware | ibm | Storwize V5000 | - | All | All | All |

| | | | | | | |
|------------------|-----|---|-----|-----|-----|-----|
| Hardware | lbn | Storwize V5000 | - | All | All | All |
| Operating System | lbn | Storwize V5000 Firmware | All | All | All | All |
| Operating System | lbn | Storwize V5000 Firmware | All | All | All | All |
| Hardware | lbn | Storwize V7000 | - | All | All | All |
| Hardware | lbn | Storwize V7000 | - | All | All | All |
| Operating System | lbn | Storwize V7000 Firmware | All | All | All | All |
| Operating System | lbn | Storwize V7000 Firmware | All | All | All | All |
| Hardware | lbn | Storwize V9000 | - | All | All | All |
| Hardware | lbn | Storwize V9000 | - | All | All | All |
| Operating System | lbn | Storwize V9000 Firmware | All | All | All | All |
| Operating System | lbn | Storwize V9000 Firmware | All | All | All | All |

References

Reference

Security Bulletin: Multiple vulnerabilities affect the IBM FlashSystem models 840 and 900

IBM X-Force Exchange

Security Bulletin: Multiple vulnerabilities affect the IBM FlashSystem model V840

Security Bulletin: Multiple vulnerabilities in IBM SAN Volume Controller, IBM Storwize, IBM Spectrum Virtualize and IBM FlashSystem product

Multiple IBM Products Multiple Security Vulnerabilities

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](#).

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

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