

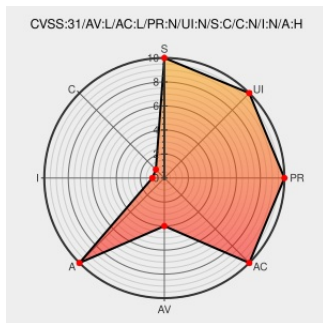


CVE-2020-4411

Published on: 05/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:22 PM UTC

CVE-2020-4411

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Aix](#) from [Ibm](#) contain the following vulnerability:

The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service vulnerability in its kernel module that could allow an attacker to cause a denial of service condition on the affected system. To exploit this vulnerability, a local attacker could invoke a subset of iocls on the Spectrum Scale device with non-valid arguments. This could allow the attacker to crash the kernel. IBM X-Force ID: 179986.

CVE-2020-4411 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [IBM](#) - **Spectrum Scale** version **4.2.0.0**

Affected Vendor/Software: [IBM](#) - **Spectrum Scale** version **5.0.0.0**

Affected Vendor/Software: [IBM](#) - **Spectrum Scale** version **5.0.4.3**

Affected Vendor/Software: [IBM](#) - **Spectrum Scale** version **4.2.3.21**

CVSS3 Score: **7.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

NONE

COMPLETE

CVE References

Description	Tags	Link
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	 XF ibm-spectrum-cve20204411-dos (179986)
Security Bulletin: A vulnerability has been identified in IBM Spectrum Scale where an unprivileged user to cause denial of service in kernel (CVE-2020-4411)	Vendor Advisory www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6209002

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	ibm	Aix	-	All	All	All
Operating System	ibm	Aix	-	All	All	All
Application	ibm	Spectrum Scale	All	All	All	All
Application	ibm	Spectrum Scale	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

cpe:2.3:o:ibm:aix:-:*:*:*:*:*:

cpe:2.3:o:ibm:aix:-:*:*:*:*:*:

cpe:2.3:a:ibm:spectrum_scale:*:*:*:*:*:

cpe:2.3:a:ibm:spectrum_scale:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023  |

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](#)