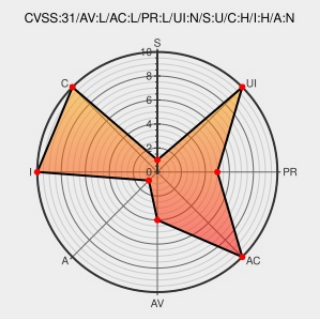
CVE-2019-4652

Published on: 11/12/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:34 PM UTC

CVE-2019-4652

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Spectrum Protect Plus from Ibm contain the following vulnerability:

IBM Spectrum Protect Plus 10.1.0 through 10.1.4 uses insecure file permissions on restored files and directories in Windows which could allow a local user to obtain sensitive information or perform unauthorized actions. IBM X-Force ID: 170963.

CVE-2019-4652 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **IBM** - **Spectrum Protect Plus** version **10.1.0**

Affected Vendor/Software: **IBM** - **Spectrum Protect Plus** version **10.1.4**

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link

IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-spectrum-cve2019-4652-file-perms (170963)
Security Bulletin: Incorrect permissions on restored files and directories on Windows using IBM Spectrum Protect Plus (CVE-2019-4652)	Vendor Advisory www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/1105683

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Spectrum Protect Plus	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

cpe:2.3:a:ibm:spectrum_protect_plus:*:*:*:*:*:*:*:*:

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→