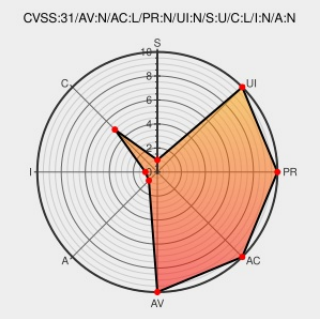
CVE-2020-4625

Published on: 11/30/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-4625

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



Certain versions of Cloud Pak For Security from Ibm contain the following vulnerability:

IBM Cloud Pak for Security 1.3.0.1(CP4S) could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie.

CVE-2020-4625 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **IBM** - **Cloud Pak for Security** version **1.3.0.1**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com	XF ibm-cp4s-cve20204625-info-disc (185360)

	text/html	
Security Bulletin: CP4S 1.3.0.1 fails to use HTTPOnly flag (CVE-2020-4625)	Patch Vendor Advisory www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6372536

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Cloud Pak For Security	1.3.0.1	All	All	All
Application	Ibm	Cloud Pak For Security	1.3.0.1	All	All	All

cpe:2.3:a:ibm:cloud_pak_for_security:1.3.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:cloud_pak_for_security:1.3.0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→