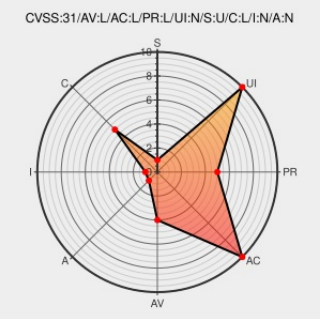
CVE-2021-20396

Published on: 06/11/2021 12:00:00 AM UTC

Last Modified on: 06/21/2021 05:42:00 PM UTC

CVE-2021-20396

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



Certain versions of Security Qradar Analyst Workflow from Ibm contain the following vulnerability:

IBM QRadar Analyst Workflow App 1.0 through 1.18.0 for IBM QRadar SIEM allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 196009.

CVE-2021-20396 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **IBM** - **QRadar Analyst Workflow** version **1.0**

Affected Vendor/Software: **IBM** - **QRadar Analyst Workflow** version **1.18.0**

CVSS3 Score: 3.3 - LOW

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-qradar-cve202120396-info-disc (196009)
Security Bulletin: IBM Security QRadar Analyst Workflow App for IBM QRadar SIEM is vulnerable to cacheable SSL Pages (CVE-2021-20396)	www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6462585

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Security Qradar Analyst Workflow	All	All	All	All

cpe:2.3:a:ibm:security_qradar_analyst_workflow:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-20396 : #IBM QRadar Analyst Workflow App 1.0 through 1.18.0 for IBM QRadar SIEM allows web pages to be sto… twitter.com/i/web/status/1…	2021-06-11 14:28:59

← Previous ID

Next ID→