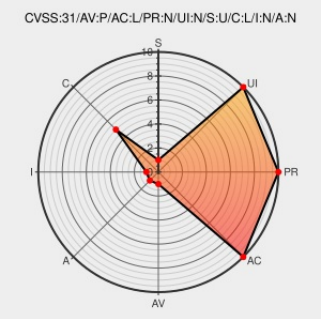
CVE-2020-4197

Published on: 03/03/2020 12:00:00 AM UTC

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

CVE-2020-4197

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



Certain versions of Tivoli Netcool/omnibus from Ibm contain the following vulnerability:

IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 174908.

CVE-2020-4197 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **IBM** - **Tivoli Netcool/OMNIbus** version **8.1.0**

CVSS3 Score: 2.4 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	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
Security Bulletin: Cacheable HTTPS Responses have been identified on multiple Tivoli Netcool/OMNIbus WebGUI admin pages (CVE-2020-4197)	Patch, Vendor Advisory, www.ibm.com	CONFIRM www.ibm.com/support/pages/node/5690822

	text/html	
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-tivoli-cve20204197-info-disc (174908)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Tivoli Netcool/omnibus	8.1.0	All	All	All
Application	Ibm	Tivoli Netcool/omnibus	8.1.0	All	All	All

cpe:2.3:a:ibm:tivoli_netcool\/omnibus:8.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:tivoli_netcool\/omnibus:8.1.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→