

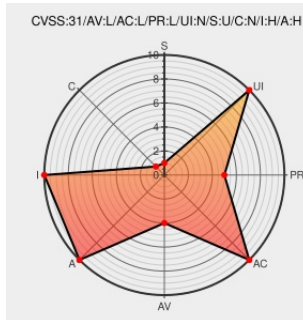


CVE-2020-5972

Published on: 06/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5972

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

Certain versions of [Virtual Gpu Manager](#) from [Nvidia](#) contain the following vulnerability:

NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which local pointer variables are not initialized and may be freed later, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).

CVE-2020-5972 has been assigned by psirt@nvidia.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **NVIDIA - NVIDIA vGPU Software** version **All**

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	NONE	HIGH	HIGH

CVSS2 Score: **3.6 - LOW**

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

CVE References

Description	Tags	Link
Security Bulletin: NVIDIA GPU Display Driver - June 2020	Vendor Advisory	CONFIRM

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nvidia	Virtual Gpu Manager	All	All	All	All
Application	Nvidia	Virtual Gpu Manager	All	All	All	All
Application	Nvidia	Virtual Gpu Manager	All	All	All	All
cpe:2.3:a:nvidia:virtual_gpu_manager:*****:						
cpe:2.3:a:nvidia:virtual_gpu_manager:*****:						
cpe:2.3:a:nvidia:virtual_gpu_manager:*****:						

Next ID→