



CVE-2020-5984

Published on: 10/02/2020 12:00:00 AM UTC

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

CVE-2020-5984

[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 it may have the use-after-free vulnerability while freeing some resources, which may lead to denial of service, code execution, and information disclosure. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.

CVE-2020-5984 has been assigned by psirt@nvidia.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **NVIDIA - NVIDIA vGPU Software** version **vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Related QID Numbers

Known Affected Configurations (CPE V2.3)

No vendor comments have been submitted for this CVE