



CVE-2021-1098

Published on: 07/20/2021 12:00:00 AM UTC

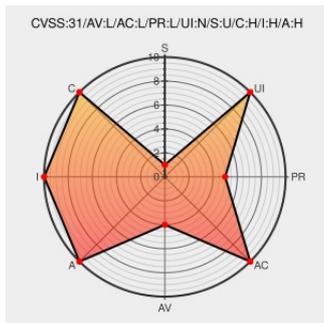
Last Modified on: 07/30/2021 01:08:00 PM UTC

CVE-2021-1098

Source: Mitre

Source: Nist

Print: PDF



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

NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it doesn't release some resources during driver unload requests from guests. This flaw allows a malicious guest to perform operations by reusing those resources, which may lead to information disclosure, data tampering, or denial of service.

This affects vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8).

CVE-2021-1098 has been assigned by psirt@nvidia.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **NVIDIA - NVIDIA Virtual GPU Software** version **vGPU version 12.x (prior to 12.3), version 11.x (prior to 11.5) and version 8.x (prior 8.8)**.

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				
Security Bulletin: NVIDIA GPU Display Drivers - July 2021 NVIDIA	nvidia.custhelp.com text/html	 CONFIRM nvidia.custhelp.com/app/answers/detail/a_id/5211				
<p>By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.</p>						
<p>There are currently no QIDs associated with this CVE</p>						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Nvidia	Virtual Gpu	All	All	All	All
<pre>cpe:2.3:a:nvidia:virtual_gpu:*:*:*:*:*:*</pre>						
<p>No vendor comments have been submitted for this CVE</p>						
Social Mentions						
Source	Title					Posted (UTC)
 @CVEreport	CVE-2021-1098 : NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager vGPU plugin , where it do... twitter.com/i/web/status/1...					2021-07-21 03:00:10
 @SecRiskRptSME	RT: CVE-2021-1098 NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it... twitter.com/i/web/status/1...					2021-07-21 07:21:25
 @threatmeter	CVE-2021-1098 NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it does... twitter.com/i/web/status/1...					2021-07-22 07:09:37
 /r/netcve	CVE-2021-1098					2021-07-21 03:38:44
← Previous ID			Next ID →			

© CVE.report 2021   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report