



CVE-2016-8805

Published on: 11/08/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:08 PM UTC

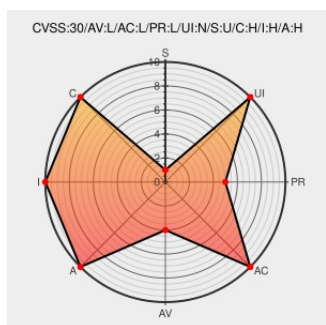
CVE-2016-8805

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x7000014 where a value passed from an user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of privileges.

CVE-2016-8805 has been assigned by psirt@nvidia.com to track the vulnerability - currently rated as **HIGH** severity.

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: **7.2 - HIGH**

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

CVE References

Description	Tags	Link
NVIDIA Driver - Stack Buffer Overflow in Escape 0x7000014 - Windows dos Exploit	Third Party Advisory VDB Entry	EXPLOIT-DB 40667

www.exploit-db.com
[Proof of Concept](#)
[text/html](#)

Security Bulletin: Vulnerabilities in NVIDIA Windows GPU Display Driver and NVIDIA GeForce Experience | NVIDIA

[Patch](#)
[Vendor Advisory](#)
nvidia.custhelp.com
[text/html](#)

 **CONFIRM**
nvidia.custhelp.com/app/answers/detail/a_id/4247

Solutions len 10822

[Third Party Advisory](#)
support.lenovo.com
[text/html](#)

 **CONFIRM**
support.lenovo.com/us/en/solutions/LEN-10822

NVIDIA GPU Display Driver CVE-2016-8805 Local Privilege Escalation Vulnerability

[Third Party Advisory](#)  [BID 94001](#)
[VDB Entry](#)
[cve.report \(archive\)](#)
[text/html](#)

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Nvidia	Gpu Driver	All	All	All	All
Application	Nvidia	Gpu Driver	All	All	All	All
cpe:2.3:o:microsoft:windows:*****:						
cpe:2.3:o:microsoft:windows:*****:						
cpe:2.3:a:nvidia:gpu_driver:*****:						
cpe:2.3:a:nvidia:gpu_driver:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)