

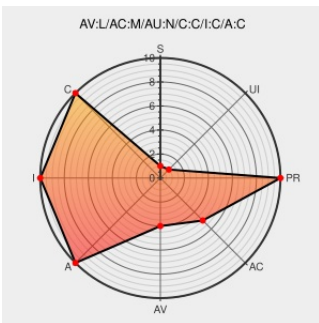


CVE-2014-5332

Published on: 02/06/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

CVE-2014-5332

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

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

Race condition in NVMap in NVIDIA Tegra Linux Kernel 3.10 allows local users to gain privileges via a crafted NVMAP_IOCTL_CREATE IOCTL call, which triggers a use-after-free error, as demonstrated by using a race condition to escape the Chrome sandbox.

CVE-2014-5332 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability

CVSS2 Score: **6.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Project Zero: Exploiting NVMAP to escape the Chrome sandbox - CVE-2014-5332

Exploit

googleprojectzero.blogspot.com

text/html

MISC

googleprojectzero.blogspot.com/2015/01/exploiting-nvmap-to-escape-chrome.html

CVE-2014-5332: TEGRA LINUX KERNEL NVMAP VULNERABILITY

Vendor Advisory

nvidia.custhelp.com

text/html

CONFIRM

nvidia.custhelp.com/app/answers/detail/a_id/3618

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	Linux	Linux Kernel	3.10	All	All	All
Operating System	Linux	Linux Kernel	3.10	All	All	All
cpe:2.3:o:linux:linux_kernel:3.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:3.10:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		