

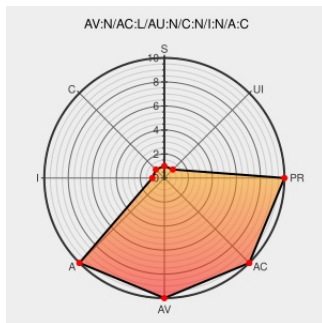


CVE-2013-7445

Published on: 10/15/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7445

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

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

The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated by JavaScript code that creates many CANVAS elements for rendering by Chrome or Firefox.

CVE-2013-7445 has been assigned by cert@cert.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Bug 60533 – CVE-2013-7445: Remote web page triggerable DOS in Linux DRM graphics.

[bugzilla.kernel.org](#)

[text/html](#)

[MISC](#)
[bugzilla.kernel.org/show_bug.cgi?id=60533](#)

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	4.0.1	All	All	All
Operating System	Linux	Linux Kernel	4.0.2	All	All	All
Operating System	Linux	Linux Kernel	4.0.3	All	All	All
Operating System	Linux	Linux Kernel	4.0.4	All	All	All
Operating System	Linux	Linux Kernel	4.0.5	All	All	All
Operating System	Linux	Linux Kernel	4.0.6	All	All	All
Operating System	Linux	Linux Kernel	4.0.7	All	All	All
Operating System	Linux	Linux Kernel	4.0.8	All	All	All
Operating System	Linux	Linux Kernel	4.0.9	All	All	All
Operating System	Linux	Linux Kernel	4.1.1	All	All	All
Operating System	Linux	Linux Kernel	4.1.10	All	All	All
Operating System	Linux	Linux Kernel	4.1.2	All	All	All
Operating System	Linux	Linux Kernel	4.1.3	All	All	All
Operating System	Linux	Linux Kernel	4.1.4	All	All	All
Operating System	Linux	Linux Kernel	4.1.5	All	All	All
Operating System	Linux	Linux Kernel	4.1.6	All	All	All
Operating System	Linux	Linux Kernel	4.1.7	All	All	All
Operating System	Linux	Linux Kernel	4.1.8	All	All	All
Operating System	Linux	Linux Kernel	4.1.9	All	All	All
Operating System	Linux	Linux Kernel	4.2.1	All	All	All
Operating System	Linux	Linux Kernel	4.2.2	All	All	All
Operating System	Linux	Linux Kernel	4.2.3	All	All	All

Operating System	Linux	Linux Kernel	4.2.3	All	All	All
Operating System	Linux	Linux Kernel	4.0.1	All	All	All
Operating System	Linux	Linux Kernel	4.0.2	All	All	All
Operating System	Linux	Linux Kernel	4.0.3	All	All	All
Operating System	Linux	Linux Kernel	4.0.4	All	All	All
Operating System	Linux	Linux Kernel	4.0.5	All	All	All
Operating System	Linux	Linux Kernel	4.0.6	All	All	All
Operating System	Linux	Linux Kernel	4.0.7	All	All	All
Operating System	Linux	Linux Kernel	4.0.8	All	All	All
Operating System	Linux	Linux Kernel	4.0.9	All	All	All
Operating System	Linux	Linux Kernel	4.1.1	All	All	All
Operating System	Linux	Linux Kernel	4.1.10	All	All	All
Operating System	Linux	Linux Kernel	4.1.2	All	All	All
Operating System	Linux	Linux Kernel	4.1.3	All	All	All
Operating System	Linux	Linux Kernel	4.1.4	All	All	All
Operating System	Linux	Linux Kernel	4.1.5	All	All	All
Operating System	Linux	Linux Kernel	4.1.6	All	All	All
Operating System	Linux	Linux Kernel	4.1.7	All	All	All
Operating System	Linux	Linux Kernel	4.1.8	All	All	All
Operating System	Linux	Linux Kernel	4.1.9	All	All	All
Operating System	Linux	Linux Kernel	4.2.1	All	All	All
Operating System	Linux	Linux Kernel	4.2.2	All	All	All
Operating System	Linux	Linux Kernel	4.2.3	All	All	All
Operating System	Linux	Linux Kernel	4.2.3	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
		cpe:2.3:o:linux:linux_kernel:4.0.1:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.2:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.3:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.4:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.5:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.6:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.7:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.8:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.9:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.1:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.10:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.2:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.3:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.4:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.5:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.6:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.7:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.8:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.1.9:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.2.1:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.2.2:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.2.3:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.1:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.2:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.3:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.4:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.5:*****:*				
		cpe:2.3:o:linux:linux_kernel:4.0.6:*****:*				

cpe:2.3:o:linux:linux_kernel:4.0.6:*****:
cpe:2.3:o:linux:linux_kernel:4.0.7:*****:
cpe:2.3:o:linux:linux_kernel:4.0.8:*****:
cpe:2.3:o:linux:linux_kernel:4.0.9:*****:
cpe:2.3:o:linux:linux_kernel:4.1.1:*****:
cpe:2.3:o:linux:linux_kernel:4.1.10:*****:
cpe:2.3:o:linux:linux_kernel:4.1.2:*****:
cpe:2.3:o:linux:linux_kernel:4.1.3:*****:
cpe:2.3:o:linux:linux_kernel:4.1.4:*****:
cpe:2.3:o:linux:linux_kernel:4.1.5:*****:
cpe:2.3:o:linux:linux_kernel:4.1.6:*****:
cpe:2.3:o:linux:linux_kernel:4.1.7:*****:
cpe:2.3:o:linux:linux_kernel:4.1.8:*****:
cpe:2.3:o:linux:linux_kernel:4.1.9:*****:
cpe:2.3:o:linux:linux_kernel:4.2.1:*****:
cpe:2.3:o:linux:linux_kernel:4.2.2:*****:
cpe:2.3:o:linux:linux_kernel:4.2.3:*****:
cpe:2.3:o:linux:linux_kernel:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)