

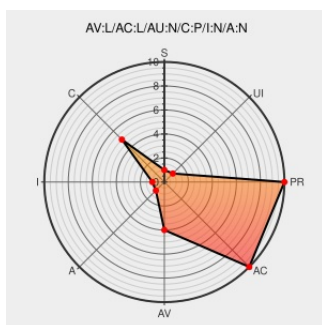


CVE-2013-2190

Published on: 10/17/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

CVE-2013-2190

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

Certain versions of [Clutter](#) from [Clutter Project](#) contain the following vulnerability:

The `translate_hierarchy_event` function in `x11/clutter-device-manager-xi2.c` in Clutter, when resuming the system, does not properly handle `XIQueryDevice` errors when a device has "disappeared," which causes the `gnome-shell` to crash and allows physically proximate attackers to access the previous `gnome-shell` session via unspecified vectors.

CVE-2013-2190 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

x11: trap errors when calling `XIQueryDevice` (d343cc62) · Commits · GNOME / clutter · GitLab

git.gnome.org
text/html

CONFIRM git.gnome.org/browse/clutter/commit/?h=clutter-1.16&id=d343cc6289583a7b0d929b82b740499ed588b1ab

980111 – (CVE-2013-2190) CVE-2013-2190 clutter: Improper translation of hierarchy events (gnome-shell crash after system resume)

bugzilla.redhat.com
text/html

CONFIRM bugzilla.redhat.com/show_bug.cgi?id=980111

x11: trap errors when calling `XIQueryDevice` (e310c68d) · Commits · GNOME / clutter · GitLab

Exploit
Patch
git.gnome.org
text/html

CONFIRM git.gnome.org/browse/clutter/commit/?h=clutter-1.14&id=e310c68d7b38d521e341f4e8a36f54303079d74e

Bug 701974 – x11: trap errors when calling `XIQueryDevice`

bugzilla.gnome.org
text/html

CONFIRM bugzilla.gnome.org/show_bug.cgi?id=701974

oss-security - Re: CVE request: gnome-shell crash, screen unlock on resume

[www.openwall.com](http://www.openwall.com/text/html)[text/html](http://www.openwall.com/text/html)

 [MLIST \[oss-security\] 20130618 Re: CVE request: gnome-shell crash, screen unlock on resume](#)

openSUSE-SU-2013:1540-1: moderate: clutter: fixed a crash after system r

[Vendor Advisory](#)[lists.opensuse.org](http://lists.opensuse.org/lists.opensuse.org/text/html)[text/html](#)

 [SUSE openSUSE-SU-2013:1540](#)

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
Application	Clutter Project	Clutter	-	All	All	All
Application	Clutter Project	Clutter	-	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
cpe:2.3:a:clutter_project:clutter:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:a:clutter_project:clutter:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:opensuse:opensuse:12.2:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:opensuse:opensuse:12.3:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:opensuse:opensuse:12.2:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:opensuse:opensuse:12.3:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

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](#)