Bug 868543 (CVE-2022-41322) - <x11-terms/kitty-0.26.2: arbitrary code execution via desktop notifications

Status:	RESOLVED FIXED	**Reported:**	2022-09-05 06:39 UTC by Carter Sande
		Modified:	2022-09-29 14:52 UTC (History)
Alias:	CVE-2022-41322	**CC List:**	3 users (show)
Product:	Gentoo Security	**See Also:**	
Component:	Vulnerabilities (show other bugs)		
Hardware:	All Linux		
Importance:	Normal normal (vote)		
Assignee:	Gentoo Security		
URL:			
Whiteboard:	B2 [glsa+]		
Keywords:			
Depends on:			
Blocks:			

Attachments		
POC text file (runs "gnome-calculator" when notification clicked) (poc.txt,49 bytes, text/plain) 2022-09-05 06:39 UTC, Carter Sande	*no flags*	Details
Add an attachment (proposed patch, testcase, etc.)		View All

Note

You need to log in before you can comment on or make changes to this bug.

Note: Please do not mark this bug as resolved after bumping or stabilizing. The Security Team will take care of that. Thanks.

Carter Sande 2022-09-05 06:39:15 UTC **Description**

Created attachment 803263 [details]
POC text file (runs "gnome-calculator" when notification clicked)

In Kitty versions 0.26.1 and below, maliciously-constructed control sequences can cause Kitty to display a notification that, when clicked, causes Kitty to execute arbitrary commands. (This could happen if someone uses "cat", "curl", or similar commands to view untrusted content in Kitty.)

The issue was fixed in Kitty version 0.26.2 and immediately disclosed in the changelog for that version.

Larry the Git Cow Dev **2022-09-05 06:59:17 UTC** **Comment 1**

The bug has been referenced in the following commit(s):

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=26e4741f77fb5a51daf4f54e234bd3d29cb27616

```
commit 26e4741f77fb5a51daf4f54e234bd3d29cb27616
Author:     Ionen Wolkens <ionen@gentoo.org>
AuthorDate: 2022-09-05 06:55:15 +0000
Commit:     Ionen Wolkens <ionen@gentoo.org>
CommitDate: 2022-09-05 06:58:36 +0000

    x11-terms/kitty: add 0.26.2

    Bug: https://bugs.gentoo.org/868543
    Signed-off-by: Ionen Wolkens <ionen@gentoo.org>

 x11-terms/kitty/Manifest             |   2 +
 x11-terms/kitty/kitty-0.26.2.ebuild | 131 ++++++++++++++++++++++++++++++++++++
 2 files changed, 133 insertions(+)
```

Ionen Wolkens Dev **2022-09-05 07:07:11 UTC** **Comment 2**

Will stable+cleanup in ~3-4 days if no issues, was already looking to stable 0.26.x soon'ish, so will go with this one instead.

Thanks for the report.

John Helmert III AT Infra Dev Sec **2022-09-05 16:42:14 UTC** **Comment 3**

Thanks for reporting! They should really indicate that this is a security release (https://github.com/kovidgoyal/kitty/releases/tag/v0.26.2), or make the security fix more noticable in the changelog

Carter Sande **2022-09-05 17:52:34 UTC** **Comment 4**

```
(In reply to John Helmert III from comment #3)
> Thanks for reporting! They should really indicate that this is a security
> release [...], or make
> the security fix more noticable in the changelog
```

Upstream's policy is not to treat security vulnerabilities differently from other types of bugs (they don't issue separate security advisories or anything), but I've emailed them to let them you about your comment.

I'd also be happy to try and request a CVE ID if you think one is warranted here.

John Helmert III AT Infra Dev Sec **2022-09-05 17:55:00 UTC** **Comment 5**

```
(In reply to Carter Sande from comment #4)
> (In reply to John Helmert III from comment #3)
> > Thanks for reporting! They should really indicate that this is a security
> > release [...], or make
> > the security fix more noticable in the changelog
>
> Upstream's policy is not to treat security vulnerabilities differently from
> other types of bugs (they don't issue separate security advisories or
> anything), but I've emailed them to let them you about your comment.
>
```

> I'd also be happy to try and request a CVE ID if you think one is warranted
> here.

Thanks! That would be very useful: https://cveform.mitre.org

Larry the Git Cow Dev **2022-09-08 18:23:44 UTC** **Comment 6**

The bug has been referenced in the following commit(s):

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=6895321462771307e2d14b334eb3ff2daf58a9d5

```
commit 6895321462771307e2d14b334eb3ff2daf58a9d5
Author:     Ionen Wolkens <ionen@gentoo.org>
AuthorDate: 2022-09-08 18:19:05 +0000
Commit:     Ionen Wolkens <ionen@gentoo.org>
CommitDate: 2022-09-08 18:23:02 +0000

    x11-terms/kitty: drop vulnerable 0.25.2, 0.26.1

    Bug: https://bugs.gentoo.org/868543
    Signed-off-by: Ionen Wolkens <ionen@gentoo.org>

 x11-terms/kitty/Manifest                          |   4 -
 x11-terms/kitty/files/kitty-0.23.1-flags.patch |  17 ----
 x11-terms/kitty/kitty-0.25.2.ebuild               | 135 -------------------------
 x11-terms/kitty/kitty-0.26.1.ebuild               | 131 ------------------------
 4 files changed, 287 deletions(-)
```

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=aae583bd5eefd64922875b05112b144c02432472

```
commit aae583bd5eefd64922875b05112b144c02432472
Author:     Ionen Wolkens <ionen@gentoo.org>
AuthorDate: 2022-09-08 18:17:39 +0000
Commit:     Ionen Wolkens <ionen@gentoo.org>
CommitDate: 2022-09-08 18:23:01 +0000

    x11-terms/kitty: stabilize 0.26.2 for amd64, x86

    Bug: https://bugs.gentoo.org/868543
    Signed-off-by: Ionen Wolkens <ionen@gentoo.org>

 x11-terms/kitty/kitty-0.26.2.ebuild | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)
```

John Helmert III AT Infra Dev Sec **2022-09-09 04:35:38 UTC** **Comment 7**

Carter, did you request a CVE?

Carter Sande **2022-09-09 04:38:28 UTC** **Comment 8**

(In reply to John Helmert III from comment #7)
> Carter, did you request a CVE?

On Sept 5, I filled out the form on Mitre's website and received a confirmation email saying I was "CVE Request 1324066". I haven't received any further communication from them.

John Helmert III AT Infra Dev Sec **2022-09-09 04:43:33 UTC** **Comment 9**

(In reply to Carter Sande from comment #8)
> (In reply to John Helmert III from comment #7)
> > Carter, did you request a CVE?
>
> On Sept 5, I filled out the form on Mitre's website and received a
> confirmation email saying I was "CVE Request 1324066". I haven't received
> any further communication from them.

Thanks! That should mean the ball is rolling, but they're not very consistent on how quickly they assign CVEs.

Carter Sande **2022-09-23 05:02:11 UTC** **Comment 10**

MITRE got back to me and said, "Use CVE-2022-41322."

John Helmert III AT Infra Dev Sec **2022-09-23 14:17:41 UTC** **Comment 11**

Thanks!

John Helmert III AT Infra Dev Sec **2022-09-26 14:03:42 UTC** **Comment 12**

GLSA request filed

Larry the Git Cow Dev **2022-09-29 14:48:24 UTC** **Comment 13**

The bug has been referenced in the following commit(s):

https://gitweb.gentoo.org/data/glsa.git/commit/?id=15167f10e54b74097a0bfd3fb525a16a7a528280

```
commit 15167f10e54b74097a0bfd3fb525a16a7a528280
Author:     GLSAMaker <glsamaker@gentoo.org>
AuthorDate: 2022-09-29 14:24:10 +0000
Commit:     John Helmert III <ajak@gentoo.org>
CommitDate: 2022-09-29 14:48:01 +0000

    [ GLSA 202209-22 ] Kitty: Arbitrary Code Execution

    Bug: https://bugs.gentoo.org/868543
    Signed-off-by: GLSAMaker <glsamaker@gentoo.org>
    Signed-off-by: John Helmert III <ajak@gentoo.org>

 glsa-202209-22.xml | 42 ++++++++++++++++++++++++++++++++++++++++++
 1 file changed, 42 insertions(+)
```

Format For Printing - XML - Clone This Bug - Clone In The Same Product - Top of page