

## Bug 868495 (CVE-2022-41138) - <x11-terms/zutty-0.13: arbitrary code execution via DECRQSS (like CVE-2008-2383)

**Status:** RESOLVED FIXED

**Reported:** 2022-09-04 20:32 UTC by Carter Sande

**Alias:** CVE-2022-41138

**Modified:** 2022-09-29 14:54 UTC ([History](#))

**CC List:** 1 user ([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:** ~~869494~~

**Blocks:**

Show dependency [tree](#)

### Attachments

<b>POC text file (runs "cat /etc/passwd" when displayed in Zutty).</b> (poc.txt,24 bytes, application/octet-stream) <a href="#">2022-09-04 20:32 UTC</a> , Carter Sande	<i>no flags</i>	<a href="#">Details</a>
<b>Patch for zutty-0.12</b> (DECRQSS-vuln.patch,291 bytes, patch) <a href="#">2022-09-05 05:43 UTC</a> , Carter Sande	<i>no flags</i>	<a href="#">Details</a>   <a href="#">Diff</a>
<a href="#">Add an attachment</a> (proposed patch, testcase, etc.)		<a href="#">View All</a>

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** 2022-09-04 20:32:34 UTC

[Description](#)

Created [attachment 803227](#) [[details](#)]

POC text file (runs "cat /etc/passwd" when displayed in Zutty)

x11-terms/zutty contains a vulnerability which allows arbitrary commands to be run by an attacker who can cause output to be sent to the terminal. Specifically, they can include newlines in an invalid DECRQSS command and Zutty will send those newlines (along with any command included) back to the shell. This vulnerability very closely resembles CVE-2008-2383 in xterm.

I have confirmed this vulnerability exists in x11-terms/zutty-0.12 in Gentoo, and I suspect it exists in all versions since 0.2 (when the code to handle DECRQSS was added).

I have not reported this issue to upstream, as I was unable to find a private method of contact. I would appreciate any help the Gentoo Security team can provide in responsibly disclosing/fixing the issue.

**Sam James**     **2022-09-04 20:38:58 UTC**

[Comment 1](#)

Thanks. Could you try emailing Tom Szilagyi <[tom.szilagyi@altmail.se](mailto:tom.szilagyi@altmail.se)>?

**Carter Sande** **2022-09-04 20:40:02 UTC**

[Comment 2](#)

(In reply to Sam James from [comment #1](#))  
> Thanks. Could you try emailing Tom Szilagyi <[tom.szilagyi@altmail.se](mailto:tom.szilagyi@altmail.se)>?

Sure thing, I've emailed him and will update this bug once I get a response.

**Carter Sande** **2022-09-05 05:43:33 UTC**

[Comment 3](#)

Created [attachment 803260](#) [[details](#), [diff](#)]  
Patch for zutty-0.12

**Carter Sande** **2022-09-05 07:25:40 UTC**

[Comment 4](#)

I talked to Tom Szilagyi via email. He hopes to have a fix for the vulnerability out by the end of the week.

**John Helmert III**     **2022-09-05 16:43:46 UTC**

[Comment 5](#)

(In reply to Carter Sande from [comment #4](#))  
> I talked to Tom Szilagyi via email. He hopes to have a fix for the  
> vulnerability out by the end of the week.

Could you go ahead and request a CVE (and ensure that MITRE knows the issue is currently private?

**Larry the Git Cow**  **2022-09-10 12:04:27 UTC**

[Comment 6](#)

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

<https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=c0388ff51cbfe987faeef5c1b10d2986e8ed8603>

commit c0388ff51cbfe987faeef5c1b10d2986e8ed8603  
Author: Matthew Smith <[matthew@gentoo.org](mailto:matthew@gentoo.org)>  
AuthorDate: 2022-09-10 12:02:47 +0000  
Commit: Matthew Smith <[matthew@gentoo.org](mailto:matthew@gentoo.org)>  
CommitDate: 2022-09-10 12:04:00 +0000

x11-terms/zutty: add 0.13

Bug: <https://bugs.gentoo.org/868495>  
Signed-off-by: Matthew Smith <[matthew@gentoo.org](mailto:matthew@gentoo.org)>

x11-terms/zutty/Manifest | 1 +  
x11-terms/zutty/zutty-0.13.ebuild | 42 +++++  
2 files changed, 43 insertions(+)

John Helmert III



2022-09-11 13:36:44 UTC

[Comment 7](#)

Please cleanup

Larry the Git Cow



2022-09-12 18:17:33 UTC

[Comment 8](#)

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

<https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=0116bc81a30a57996e71f92c190a79d0a40a001f>

```
commit 0116bc81a30a57996e71f92c190a79d0a40a001f
Author: Matthew Smith <matthew@gentoo.org>
AuthorDate: 2022-09-12 18:14:38 +0000
Commit: Matthew Smith <matthew@gentoo.org>
CommitDate: 2022-09-12 18:17:03 +0000
```

x11-terms/zutty: remove 0.12, security cleanup

Bug: <https://bugs.gentoo.org/868495>

Signed-off-by: Matthew Smith <[matthew@gentoo.org](mailto:matthew@gentoo.org)>

```
x11-terms/zutty/Manifest          | 1 -
x11-terms/zutty/zutty-0.12.ebuild | 41 -----
2 files changed, 42 deletions(-)
```

John Helmert III



2022-09-12 18:19:53 UTC

[Comment 9](#)

Thanks!

John Helmert III



2022-09-19 20:45:05 UTC

[Comment 10](#)

CVE requested

John Helmert III



2022-09-26 13:56:19 UTC

[Comment 11](#)

GLSA request filed

Larry the Git Cow



2022-09-29 14:48:38 UTC

[Comment 12](#)

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

<https://gitweb.gentoo.org/data/glsa.git/commit/?id=fc10c987b6e59d6274fa1c863e8c2c3e80119e97>

```
commit fc10c987b6e59d6274fa1c863e8c2c3e80119e97
Author: GLSAMaker <glmaker@gentoo.org>
AuthorDate: 2022-09-29 14:24:54 +0000
Commit: John Helmert III <ajak@gentoo.org>
CommitDate: 2022-09-29 14:48:02 +0000
```

[ GLSA 202209-25 ] Zutty: Arbitrary Code Execution

Bug: <https://bugs.gentoo.org/868495>

Signed-off-by: GLSAMaker <[glmaker@gentoo.org](mailto:glmaker@gentoo.org)>

Signed-off-by: John Helmert III <[ajak@gentoo.org](mailto:ajak@gentoo.org)>

glsa-202209-25.xml | 42 +++++  
1 file changed, 42 insertions(+)

**John Helmert III**



**2022-09-29 14:54:38 UTC**

[Comment 13](#)

GLSA released, all done!

---

[Format For Printing](#) - [XML](#) - [Clone This Bug](#) - [Clone In The Same Product](#) - [Top of page](#)