Message-ID: <CAP9KPhBoGPeqbjyVaEp84kBFMg09do0YEf_Le2vFOO3faS7oJQ@mail.gmail.com>
Date: Mon, 17 Jun 2024 11:48:59 +1000
From: David Leadbeater <dgl@....cx>
To: oss-security@...ts.openwall.com
Cc: George Nachman <gnachman@...il.com>, Vinci <vinci@...tonmail.ch>
Subject: Re: iTerm2 3.5.x title reporting bug

Hi,

On Sat, 15 Jun 2024 at 11:37, David Leadbeater <dgl@....cx> wrote:
[...]
> This is not trivially exploitable (at least in a way that works
> without user interaction), as it is not possible to echoback a newline
> or control characters. However as Zsh is the default shell on macOS it
> may be possible to use some of the vi techniques like I used in xterm
> CVE-2022-45063[1]. Some of the techniques in solid-snail's previous
> iTerm2 research[2] could apply too. So treat this as potential remote
> code execution.

I spoke too soon, this was independently discovered by Vin01 -- along
with a tmux integration issue. The additional finding by Vin01 allows
for remote code execution via the tmux escape sequence (as it allows a
newline to be inserted).

Their write up is available from
https://vin01.github.io/piptagole/escape-sequences/iterm2/rce/2024/06/16/iterm2-rce-window-title-tmux-integration.html

There are now two CVEs assigned:
- CVE-2024-38395 (title reporting, the original issue reported)
- CVE-2024-38396 (tmux integration, combined with title reporting)

The second commit (fc60236a) mentioned in the post is not yet part of
an iTerm2 release. Fixing the title reporting makes this harder to
exploit but fc60236a can be considered additional hardening for the
Tmux integration.

David

Copy of the above blog post for the archives, with minor reformatting,
all credit to Vin01:

Abusing title reporting and tmux integration in iTerm2 for code execution
Jun 16, 2024

Regression turned into RCE

I am skipping an introduction to escape sequences here as I recently
wrote more about them in my previous post[1]. From a security
perspective, they are to terminal emulators what XSS is to browsers.

This post is about a new bug which affects only iTerm2 3.5.0 and 3.5.1
(released on May 20 and June 11 respectively) because of a regression.

In versions prior to 3.5.0, window title reporting was disabled. So
you could not just use following to retrieve the title of terminal
window and put it in stdin.

$ echo -e "\e]21t"

Note: David Leadbeater also independently noticed this regression and
reported it here [this thread]

What is wrong with window title reporting?

```
Ps 2[2] escape sequence allows setting the window title.

An example:

$ echo -e "\033]0;This is the window title\a"

CSI Ps 21 t can be used to retrieve that title and put it in stdin as
shown above. This makes exploitation very easy as at this point, all
that is required is for the user to hit Enter and arbitrary code
present in that title will happily execute itself.

Patch that disables title reporting by default: f1e89f78[4]

## Tmux integration made it worse

Native tmux integration (enabled by default) in iTerm2 had a weakness
which allowed sneaking in the reported title and also provided a way
to send newlines after the title was reported.

Patch: fc60236a[5]

## Can I haz that sweet PoC plz?

try this out yourself:

docker run --rm  vin01/escape-seq-test:cve-2024-38396

or

cat poc-iterm2-rce.txt

Download poc-iterm2-rce.txt[6]

The file contains this payload \033]2;s&open -aCalculator&\a\033[21t
\x1bP1000p%session-changed s which sets s&open -aCalculator& as window
title and then retrieves it back to execute and pop a calculator.

Source code: https://github.com/vin01/poc-cve-2024-38396

## A fix released within 2 days of reporting

Upgrade to iTerm2 3.5.2: https://iterm2.com/downloads.html

Please think twice before you enable Terminal may report window title
setting in iTerm2. It might not be worth the security risk as it
allows arbitrary text to end up in stdin which is never a good idea.

[1]: https://vin01.github.io/piptagole/escape-sequences/iterm2/hyper/url-handlers/code-
execution/2024/05/21/arbitrary-url-schemes-terminal-emulators.html
[2]: https://www.x.org/docs/xterm/ctlseqs.pdf [blog links to the pdf;
https://invisible-island.net/xterm/ctlseqs/ctlseqs.html is a newer
HTML version of the xterm control sequence documentation]
[3]: https://gist.github.com/halcyon/334da650816876d7be4d1bee8a157f25#file-gistfile1-txt-L872
[4]: https://gitlab.com/gnachman/iterm2/-/commit/f1e89f78dd72dcac3ba66d3d6f93db3f7f649219
[5]: https://gitlab.com/gnachman/iterm2/-/commit/fc60236a914d63fb70a5c632e211203a4f1bd4dd
[6]: https://vin01.github.io/piptagole/assets/poc-iterm2-rce.txt
```