Message-ID: <CAP9KPhArz3KdnA1szCTwE9WVrepdM4f7DiPs2hmMSa74NNzdUg@mail.gmail.com>
Date: Sat, 15 Jun 2024 11:37:39 +1000
From: David Leadbeater <dgl@....cx>
To: oss-security@...ts.openwall.com
Cc: George Nachman <gnachman@...il.com>
Subject: iTerm2 3.5.x title reporting bug

Hi,

I discovered iTerm2 versions 3.5.0 and 3.5.1 (and some beta versions)
have a bug where the preference for whether title reporting is enabled
is not respected -- the result is title reporting is always enabled*.

This is fixed by iTerm2 3.5.2, available from
https://iterm2.com/downloads.html -- automatic updates should prompt
you to install this version. There is no CVE yet, this is essentially
another variant of CVE-2003-0063...

To test if you're vulnerable:
printf '\e]0;ivulnerable\a\e[21t'

If you have some of all of the string "vulnerable" (but not just "l")
in your input buffer, you're vulnerable. (You can also test via ssh
termtest.dgl.cx, which does a variant of the above test and others
over SSH, source code at https://github.com/dgl/vt-houdini.)

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.

David

*: Unless you change the advanced setting "Disable potentially
insecure escape sequences" -- which works as a mitigation too, but
disables shell integration and some other features.

[1]: https://www.openwall.com/lists/oss-security/2022/11/10/1
[2]: https://blog.solidsnail.com/posts/2023-08-28-iterm2-rce