Message-ID: <Y21BdMJyg9QUm2Qw@zuma.herrb.net>
Date: Thu, 10 Nov 2022 18:22:44 +0000
From: Matthieu Herrb <matthieu@...rb.eu>
To: oss-security@...ts.openwall.com
Subject: Re: CVE-2022-45063: xterm <375 code execution via
 font ops

On Thu, Nov 10, 2022 at 02:42:41PM +1100, David Leadbeater wrote:
> xterm before patch 375 can enable an RCE under certain conditions.
>
> Fix:
>
> Upgrade to xterm patch #375
> https://invisible-island.net/xterm/xterm.log.html
>
> Mitigation:
>
> Set this Xresource:
> XTerm*allowFontOps: false

Hi,

Running xterm 375 on Arch Linux (Font Ops are enabled by default) and
OpenBSD (after re-enabling Font Ops) shows it as still vulnerable
using the test below..

>
> Details:
>
> The issue is in the OSC 50 sequence, which is for setting and querying
> the font. If a given font does not exist, it is not set, but a query
> will return the name that was set. Control characters can't be
> included, but the response string can be terminated with ^G. This
> essentially gives us a primitive for echoing text back to the terminal
> and ending it with ^G.
>
> It so happens ^G is in Zsh when in vi line editing mode bound to
> "list-expand". Which can run commands as part of the expansion leading
> to command execution without pressing enter!
>
> This does mean to exploit this vulnerability the user needs to be
> using Zsh in vi line editing mode (usually via $EDITOR having "vi" in
> it). While somewhat obscure this is not a totally unknown
> configuration.
>
> In that configuration, something like:
> printf "\e]50;i\$(touch /tmp/hack-like-its-1999)\a\e]50;?\a" > cve-2022-45063
> cat cve-2022-45063 # or another way to deliver this to the victim
>
> Will touch that file. It will leave the line on the user's screen;
> I'll leave it as an exercise for the reader to use the vi line editing
> commands to hide the evidence.
>
> Debian, Red Hat and others disable font ops by default (see some
> good foresight at[1] or this very list[2]), but users can re-enable them
> via a configuration option or menu. Additionally upstream xterm does
> not disable them by default, so some distributions include a
> vulnerable default configuration.
>
> This has been assigned CVE-2022-45063.
>
> David
>
>
> [1]: https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=510030

```
> [2]: https://www.openwall.com/lists/oss-security/2015/09/20/2 towards the end.

--
Matthieu Herrb
```