Readme file

===========

Gitlab exploit was performed on CentOS:

[tmp]$ uname -a

Linux localhost.localdomain 3.10.0-1160.el7.x86\_64 #1 SMP Mon Oct 19 16:18:59 UTC 2020 x86\_64 x86\_64 x86\_64 GNU/Linux

With Gitlab CE version 13.10.2 EL7

Python scripts to generate jpg-DjVu payload:

payload\_tn.sh - creates jpg image with DjVu header to invoke telnet connection to attacker VM using pipe I/O redirection

payload\_TREX.sh - creates jpg image with DjVu header to invoke TOUCH\_ME\_NOT\_TREX binary for reverse shell exploit

gen-payload-py.sh - original jpg image creation shell

jpgimages.tar - tar archive of generated jpg images for exploit during demo

Other files:

DEMO PORK CHOP.txt - sequence for demo with commands

Repository for Gitlab vulnerable version:

<https://packages.gitlab.com/app/gitlab/gitlab-ce/search?q=gitlab-ce-13.10.2>

README - this file