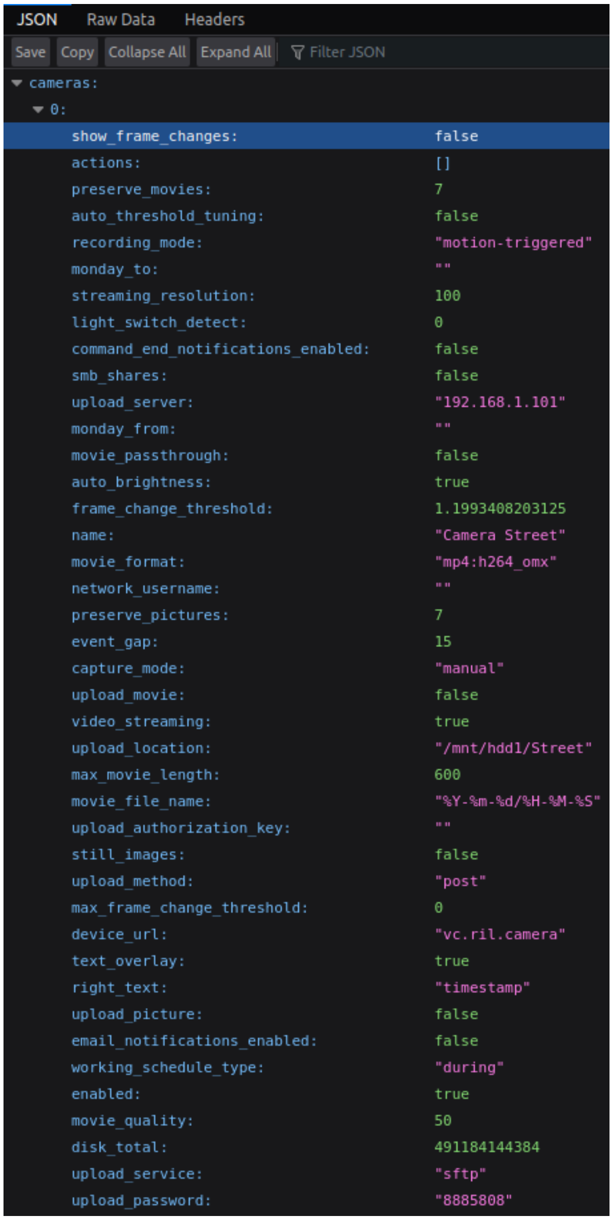
Pizza-Powered Hacking 🍕

MotionEye Config Info Disclosure

Edit: This was given CVE-2022-25568. As mentioned in my previous posts here and here, I've done a little digging into the conditions that are required for the MotioneEye config file to be world viewable, and I've reached this conclusion:

As long as a "user" password is not set, the config file will be world readable. Even if an "admin" password has been set, the /config/list file will still be readable by everybody. So, while someone could think they are doing the correct thing by creating a password for the admin user, they may still be leaking private information. Here is a innocuous example from a live instance:



```
▾ cameras:
  ▾ 0:
      show_frame_changes:                 false
      actions:                            []
      preserve_movies:                    7
      auto_threshold_tuning:              false
      recording_mode:                     "motion-triggered"
      monday_to:                          ""
      streaming_resolution:               100
      light_switch_detect:                0
      command_end_notifications_enabled:  false
      smb_shares:                         false
      upload_server:                      "192.168.1.101"
      monday_from:                        ""
      movie_passthrough:                  false
      auto_brightness:                    true
      frame_change_threshold:             1.1993408203125
      name:                               "Camera Street"
      movie_format:                       "mp4:h264_omx"
      network_username:                   ""
      preserve_pictures:                  7
      event_gap:                          15
      capture_mode:                       "manual"
      upload_movie:                       false
      video_streaming:                    true
      upload_location:                    "/mnt/hdd1/Street"
      max_movie_length:                   600
      movie_file_name:                    "%Y-%m-%d/%H-%M-%S"
      upload_authorization_key:           ""
      still_images:                       false
      upload_method:                      "post"
      max_frame_change_threshold:         0
      device_url:                         "vc.ril.camera"
      text_overlay:                       true
      right_text:                         "timestamp"
      upload_picture:                     false
      email_notifications_enabled:        false
      working_schedule_type:              "during"
      enabled:                            true
      movie_quality:                      50
      disk_total:                         491184144384
      upload_service:                     "sftp"
      upload_password:                    "8885808"
```

As you can see in this picture, IP addresses/services/passwords are exposed. This is a rather innocuous example, being that it is an internal IP address, but it illustrates how this could be an issue. Imagine if those were your public FTP server credentials. Or if they were your gmail credentials for smtp notifications. The list goes on.

Along with usernames, passwords, auth keys, and email addresses, these config files also contain less sensitive information like internal network IP addresses and URLs, drive and mounting information.

In many ways this vulnerability may be worse that the MotionEye RCE vulnerability that I reported and received a CVE for. In that case, the admin password needed to be left blank (or easily guessed) for someone to get into the admin panel and achieve RCE. In this case, a user could think they're being secure by setting an admin password, but they leave the user password blank – and the config remains viewable.

I've found gmail, gdrive, ftp, sftp, telegram stuff (not sure how auth works there), etc. all exposed to the WWW in these files.

I've submitted an issue on the MotionEye github page, but if it is anything like last time, they don't plan on fixing it/see it as a non-issue.

Edit: The issue was closed before I even finished this post.

Edit: The issue was reopened and I submitted a pull request to fix the issue, although my fix was not tested much, so it may not work properly.

This entry was posted in blog, coding, webdev, CVE, cybersecurity, hacking, infosec and tagged CVE, cyber, hacking, infosec, self hosting on February 17, 2022 [https://www.pizzapower.me/2022/02/17/motioneye-config-info-disclosure/] .