# CVE Detail – CVE-2022-24730

Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 1.3.0 but before versions 2.1.11, 2.2.6, and 2.3.0 is vulnerable to a path traversal bug, compounded by an improper access control bug, allowing a malicious user with read-only repository access to leak sensitive files from Argo CD's repo-server. A malicious Argo CD user who has been granted `get` access for a repository containing a Helm chart can craft an API request to the `/api/v1/repositories/{repo\_url}/appdetails` endpoint to leak the contents of out-of-bounds files from the repo-server. The malicious payload would reference an out-of-bounds file, and the contents of that file would be returned as part of the response. Contents from a non-YAML file may be returned as part of an error message. The attacker would have to know or guess the location of the target file. Sensitive files which could be leaked include files from other Applications' source repositories or any secrets which have been mounted as files on the repo-server. This vulnerability is patched in Argo CD versions 2.1.11, 2.2.6, and 2.3.0. The patches prevent path traversal and limit access to users who either A) have been granted Application `create` privileges or B) have been granted Application `get` privileges and are requesting details for a `repo\_url` that has already been used for the given Application. There are currently no known workarounds.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.49817

## CVSS Scoring

CVSS v3.1 Score: 7.7

Severity: HIGH

## Mapped CWE(s)

* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
* CWE-284: Improper Access Control
* CWE-863: Incorrect Authorization

## CAPEC(s)

* CAPEC-126: Path Traversal
* CAPEC-19: Embedding Scripts within Scripts
* CAPEC-441: Malicious Logic Insertion
* CAPEC-478: Modification of Windows Service Configuration
* CAPEC-479: Malicious Root Certificate
* CAPEC-502: Intent Spoof
* CAPEC-503: WebView Exposure
* CAPEC-536: Data Injected During Configuration
* CAPEC-546: Incomplete Data Deletion in a Multi-Tenant Environment
* CAPEC-550: Install New Service
* CAPEC-551: Modify Existing Service
* CAPEC-552: Install Rootkit
* CAPEC-556: Replace File Extension Handlers
* CAPEC-558: Replace Trusted Executable
* CAPEC-562: Modify Shared File
* CAPEC-563: Add Malicious File to Shared Webroot
* CAPEC-564: Run Software at Logon
* CAPEC-578: Disable Security Software
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding

## ATT&CK Techniques

* T1037: Boot or Logon Initialization Scripts
* T1027.009: Embedded Payloads
* T1014: Rootkit
* T1543: Create or Modify System Process
* T1574.011: Services Registry Permissions Weakness
* T1542.003: Bootkit
* T1547: Boot or Logon Autostart Execution
* T1080: Taint Shared Content
* T1562.009: Safe Mode Boot
* T1543.003: Windows Service
* T1505.005: Terminal Services DLL
* T1562.002: Disable Windows Event Logging
* T1562.004: Disable or Modify System Firewall
* T1543.004: Launch Daemon
* T1546.008: Accessibility Features
* T1562.007: Disable or Modify Cloud Firewall
* T1546.001: Change Default File Association
* T1547.006: Kernel Modules and Extensions
* T1562.001: Disable or Modify Tools
* T1556.006: Multi-Factor Authentication
* T1546.004: Unix Shell Configuration Modification
* T1553.004: Install Root Certificate
* T1562.008: Disable or Modify Cloud Logs
* T1543.001: Launch Agent
* T1546.016: Installer Packages

## Used By (Actors/Tools)

* HDoor (malware)
* TrickBot (malware)
* EKANS (malware)
* Ninja (malware)
* Pikabot (malware)
* Wiarp (malware)
* Exaramel for Windows (malware)
* Stuxnet (malware)
* RotaJakiro (malware)
* AvosLocker (malware)
* RobbinHood (malware)
* TDTESS (malware)
* COATHANGER (malware)
* Misdat (malware)
* Linux Rabbit (malware)
* Emissary (malware)
* Exaramel for Linux (malware)
* Ursnif (malware)
* ThreatNeedle (malware)
* RansomHub (malware)
* ZLib (malware)
* Miner-C (malware)
* LITTLELAMB.WOOLTEA (malware)
* Bankshot (malware)
* StrongPity (malware)
* xCaon (malware)
* Nebulae (malware)
* AuditCred (malware)
* Kasidet (malware)
* Hannotog (malware)
* Brave Prince (malware)
* RainyDay (malware)
* macOS.OSAMiner (malware)
* NETWIRE (malware)
* PyDCrypt (malware)
* CosmicDuke (malware)
* SslMM (malware)
* IMAPLoader (malware)
* GreyEnergy (malware)
* Emotet (malware)
* BOLDMOVE (malware)
* TEARDROP (malware)
* DUSTTRAP (malware)
* BADHATCH (malware)
* DUSTPAN (malware)
* PingPull (malware)
* Dacls (malware)
* Umbreon (malware)
* ShrinkLocker (malware)
* Hildegard (malware)
* BlackByte 2.0 Ransomware (malware)
* SUGARUSH (malware)
* HOPLIGHT (malware)
* Cuckoo Stealer (malware)
* WastedLocker (malware)
* Moneybird (malware)
* InvisiMole (malware)
* Naid (malware)
* Volgmer (malware)
* WhisperGate (malware)
* FruitFly (malware)
* ZeroT (malware)
* Keydnap (malware)
* RDAT (malware)
* Hacking Team UEFI Rootkit (malware)
* Skidmap (malware)
* Okrum (malware)
* Line Dancer (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Diavol (malware)
* IcedID (malware)
* Kazuar (malware)
* DarkComet (malware)
* CHIMNEYSWEEP (malware)
* Ragnar Locker (malware)
* BlackEnergy (malware)
* zwShell (malware)
* Zeroaccess (malware)
* DCSrv (malware)
* ShimRat (malware)
* Avaddon (malware)
* Conficker (malware)
* Green Lambert (malware)
* LockerGoga (malware)
* KeyBoy (malware)
* Anchor (malware)
* RunningRAT (malware)
* Babuk (malware)
* Dyre (malware)
* BBSRAT (malware)
* PlugX (malware)
* Reaver (malware)
* Bisonal (malware)
* MultiLayer Wiper (malware)
* Lumma Stealer (malware)
* Duqu (malware)
* Remsec (malware)
* Cuba (malware)
* Clambling (malware)
* DarkGate (malware)
* NanHaiShu (malware)
* LockBit 3.0 (malware)
* ThiefQuest (malware)
* Hydraq (malware)
* Caterpillar WebShell (malware)
* Netwalker (malware)
* Elise (malware)
* WannaCry (malware)
* Briba (malware)
* TYPEFRAME (malware)
* Bundlore (malware)
* SMOKEDHAM (malware)
* Uroburos (malware)
* Metamorfo (malware)
* PipeMon (malware)
* KONNI (malware)
* Winnti for Linux (malware)
* gh0st RAT (malware)
* Shamoon (malware)
* JHUHUGIT (malware)
* BPFDoor (malware)
* Black Basta (malware)
* Catchamas (malware)
* Attor (malware)
* MegaCortex (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* Akira \_v2 (malware)
* RTM (malware)
* BlackByte Ransomware (malware)
* Hikit (malware)
* Grandoreiro (malware)
* Sakula (malware)
* RawPOS (malware)
* Drovorub (malware)
* Bazar (malware)
* XLoader (malware)
* BADCALL (malware)
* hcdLoader (malware)
* Nidiran (malware)
* MoonWind (malware)
* Ryuk (malware)
* HermeticWiper (malware)
* Pysa (malware)
* LockBit 2.0 (malware)
* Pandora (malware)
* FinFisher (malware)
* LunarMail (malware)
* CrossRAT (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Wingbird (malware)
* Unknown Logger (malware)
* REvil (malware)
* Samurai (malware)
* OSX\_OCEANLOTUS.D (malware)
* Cyclops Blink (malware)
* PoisonIvy (malware)
* Seasalt (malware)
* NanoCore (malware)
* Carbon (malware)
* LoJax (malware)
* Calisto (malware)
* GoldenSpy (malware)
* Gold Dragon (malware)
* Ramsay (malware)
* Carberp (malware)
* HARDRAIN (malware)
* MacMa (malware)
* FunnyDream (malware)
* SysUpdate (malware)
* TinyZBot (malware)
* Kwampirs (malware)
* Nerex (malware)
* DEADEYE (malware)
* Proton (malware)
* Mango (malware)
* InnaputRAT (malware)
* Clop (malware)
* ROCKBOOT (malware)
* Egregor (malware)
* ZxShell (malware)
* CoinTicker (malware)
* Winnti for Windows (malware)
* Ebury (malware)
* Meteor (malware)
* njRAT (malware)
* ZIPLINE (malware)
* Maze (malware)
* BOOTRASH (malware)
* ComRAT (malware)
* ChChes (malware)
* JPIN (malware)
* KOCTOPUS (malware)
* Mis-Type (malware)
* XCSSET (malware)
* AppleJeus (malware)
* STARWHALE (malware)
* Industroyer (malware)
* HIDEDRV (malware)
* CozyCar (malware)
* Agent Tesla (malware)
* POWERSTATS (malware)
* Goopy (malware)
* QakBot (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* Komplex (malware)
* DEADWOOD (malware)
* Dok (malware)
* MacSpy (malware)
* Dtrack (malware)
* H1N1 (malware)
* SLOWPULSE (malware)
* LoudMiner (malware)
* BitPaymer (malware)
* BACKSPACE (malware)
* HiddenWasp (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* FALLCHILL (malware)
* certutil (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Pacu (tool)
* AADInternals (tool)
* Empire (tool)
* netsh (tool)
* Imminent Monitor (tool)
* Donut (tool)
* Invoke-PSImage (tool)
* HTRAN (tool)
* Wevtutil (tool)
* PsExec (tool)
* Indrik Spider (intrusion-set)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* APT41 DUST (campaign)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* TA505 (intrusion-set)
* APT42 (intrusion-set)
* Earth Lusca (intrusion-set)
* Operation CuckooBees (campaign)
* Play (intrusion-set)
* TA577 (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* FIN6 (intrusion-set)
* APT28 (intrusion-set)
* Cinnamon Tempest (intrusion-set)
* Darkhotel (intrusion-set)
* Ke3chang (intrusion-set)
* Magic Hound (intrusion-set)
* APT29 (intrusion-set)
* Operation Honeybee (campaign)
* 2016 Ukraine Electric Power Attack (campaign)
* Cobalt Group (intrusion-set)
* MuddyWater (intrusion-set)
* APT38 (intrusion-set)
* APT32 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* Kimsuky (intrusion-set)
* Akira (intrusion-set)
* TA2541 (intrusion-set)
* ToddyCat (intrusion-set)
* Tropic Trooper (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* APT19 (intrusion-set)
* Moses Staff (intrusion-set)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* INC Ransom (intrusion-set)
* Winnti Group (intrusion-set)
* Rocke (intrusion-set)
* Saint Bear (intrusion-set)
* Scattered Spider (intrusion-set)
* Blue Mockingbird (intrusion-set)
* RedCurl (intrusion-set)
* Gorgon Group (intrusion-set)
* C0021 (campaign)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* APT28 Nearest Neighbor Campaign (campaign)
* Gamaredon Group (intrusion-set)
* Night Dragon (campaign)
* Agrius (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* Moonstone Sleet (intrusion-set)
* Salt Typhoon (intrusion-set)
* ShadowRay (campaign)
* Axiom (intrusion-set)
* APT3 (intrusion-set)
* Putter Panda (intrusion-set)
* HomeLand Justice (campaign)
* Cutting Edge (campaign)
* Lotus Blossom (intrusion-set)
* Carbanak (intrusion-set)
* Deep Panda (intrusion-set)
* KV Botnet Activity (campaign)
* PROMETHIUM (intrusion-set)

## Affected Products

* cpe:2.3:a:argoproj:argo\_cd:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:argoproj:argo\_cd:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:argoproj:argo\_cd:2.3.0:rc1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:argoproj:argo\_cd:2.3.0:rc2:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:argoproj:argo\_cd:2.3.0:rc4:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:argoproj:argo\_cd:2.3.0:rc5:\*:\*:\*:\*:\*:\*