# CVE Detail – CVE-2022-21668

pipenv is a Python development workflow tool. Starting with version 2018.10.9 and prior to version 2022.1.8, a flaw in pipenv's parsing of requirements files allows an attacker to insert a specially crafted string inside a comment anywhere within a requirements.txt file, which will cause victims who use pipenv to install the requirements file to download dependencies from a package index server controlled by the attacker. By embedding malicious code in packages served from their malicious index server, the attacker can trigger arbitrary remote code execution (RCE) on the victims' systems. If an attacker is able to hide a malicious `--index-url` option in a requirements file that a victim installs with pipenv, the attacker can embed arbitrary malicious code in packages served from their malicious index server that will be executed on the victim's host during installation (remote code execution/RCE). When pip installs from a source distribution, any code in the setup.py is executed by the install process. This issue is patched in version 2022.1.8. The GitHub Security Advisory contains more information about this vulnerability.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.80799

## CVSS Scoring

CVSS v3.1 Score: 8.0

Severity: HIGH

## Mapped CWE(s)

* CWE-1284: Improper Validation of Specified Quantity in Input
* CWE-190: Integer Overflow or Wraparound
* CWE-20: Improper Input Validation
* CWE-427: Uncontrolled Search Path Element
* CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')
* CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
* CWE-791: Incomplete Filtering of Special Elements

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-101: Server Side Include (SSI) Injection
* CAPEC-104: Cross Zone Scripting
* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-109: Object Relational Mapping Injection
* CAPEC-110: SQL Injection through SOAP Parameter Tampering
* CAPEC-120: Double Encoding
* CAPEC-13: Subverting Environment Variable Values
* CAPEC-135: Format String Injection
* CAPEC-136: LDAP Injection
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-15: Command Delimiters
* CAPEC-153: Input Data Manipulation
* CAPEC-182: Flash Injection
* CAPEC-183: IMAP/SMTP Command Injection
* CAPEC-209: XSS Using MIME Type Mismatch
* CAPEC-22: Exploiting Trust in Client
* CAPEC-23: File Content Injection
* CAPEC-230: Serialized Data with Nested Payloads
* CAPEC-231: Oversized Serialized Data Payloads
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-248: Command Injection
* CAPEC-250: XML Injection
* CAPEC-261: Fuzzing for garnering other adjacent user/sensitive data
* CAPEC-267: Leverage Alternate Encoding
* CAPEC-28: Fuzzing
* CAPEC-3: Using Leading 'Ghost' Character Sequences to Bypass Input Filters
* CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies
* CAPEC-38: Leveraging/Manipulating Configuration File Search Paths
* CAPEC-40: Manipulating Writeable Terminal Devices
* CAPEC-42: MIME Conversion
* CAPEC-43: Exploiting Multiple Input Interpretation Layers
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-471: Search Order Hijacking
* CAPEC-473: Signature Spoof
* CAPEC-52: Embedding NULL Bytes
* CAPEC-53: Postfix, Null Terminate, and Backslash
* CAPEC-588: DOM-Based XSS
* CAPEC-6: Argument Injection
* CAPEC-63: Cross-Site Scripting (XSS)
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-664: Server Side Request Forgery
* CAPEC-67: String Format Overflow in syslog()
* CAPEC-7: Blind SQL Injection
* CAPEC-71: Using Unicode Encoding to Bypass Validation Logic
* CAPEC-72: URL Encoding
* CAPEC-73: User-Controlled Filename
* CAPEC-75: Manipulating Writeable Configuration Files
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-80: Using UTF-8 Encoding to Bypass Validation Logic
* CAPEC-81: Web Server Logs Tampering
* CAPEC-83: XPath Injection
* CAPEC-85: AJAX Footprinting
* CAPEC-88: OS Command Injection
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities
* CAPEC-92: Forced Integer Overflow

## ATT&CK Techniques

* T1574.007: Path Interception by PATH Environment Variable
* T1539: Steal Web Session Cookie
* T1574.001: DLL
* T1553.002: Code Signing
* T1574.008: Path Interception by Search Order Hijacking
* T1574.006: Dynamic Linker Hijacking
* T1562.003: Impair Command History Logging
* T1027: Obfuscated Files or Information
* T1036.001: Invalid Code Signature
* T1574.009: Path Interception by Unquoted Path
* T1574.004: Dylib Hijacking

## Used By (Actors/Tools)

* TrickBot (malware)
* EKANS (malware)
* BLINDINGCAN (malware)
* Ninja (malware)
* RCSession (malware)
* SynAck (malware)
* Bumblebee (malware)
* Amadey (malware)
* Orz (malware)
* NOKKI (malware)
* Stuxnet (malware)
* Downdelph (malware)
* AvosLocker (malware)
* Chinoxy (malware)
* COATHANGER (malware)
* Sardonic (malware)
* WindTail (malware)
* RedLeaves (malware)
* Matryoshka (malware)
* WEBC2 (malware)
* StrongPity (malware)
* Nebulae (malware)
* Janicab (malware)
* RainyDay (malware)
* Ecipekac (malware)
* AppleSeed (malware)
* BUSHWALK (malware)
* NETWIRE (malware)
* OLDBAIT (malware)
* GreyEnergy (malware)
* TEARDROP (malware)
* Turian (malware)
* Action RAT (malware)
* Prikormka (malware)
* Gootloader (malware)
* PolyglotDuke (malware)
* Hildegard (malware)
* SombRAT (malware)
* Snip3 (malware)
* LoFiSe (malware)
* WastedLocker (malware)
* RegDuke (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* ZeroT (malware)
* TRANSLATEXT (malware)
* Regin (malware)
* Line Dancer (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Diavol (malware)
* Siloscape (malware)
* Kazuar (malware)
* HUI Loader (malware)
* CHIMNEYSWEEP (malware)
* FatDuke (malware)
* DRATzarus (malware)
* BOOSTWRITE (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* Conficker (malware)
* Flagpro (malware)
* SpicyOmelette (malware)
* Green Lambert (malware)
* LockerGoga (malware)
* ISMInjector (malware)
* PUNCHBUGGY (malware)
* POSHSPY (malware)
* MiniDuke (malware)
* HyperBro (malware)
* Anchor (malware)
* DarkTortilla (malware)
* ROKRAT (malware)
* CORESHELL (malware)
* Javali (malware)
* BBSRAT (malware)
* PlugX (malware)
* Lumma Stealer (malware)
* DustySky (malware)
* Epic (malware)
* Cuba (malware)
* Clambling (malware)
* DarkGate (malware)
* SVCReady (malware)
* FoggyWeb (malware)
* Carbanak (malware)
* XTunnel (malware)
* Hydraq (malware)
* Gazer (malware)
* Saint Bot (malware)
* Chaes (malware)
* Bundlore (malware)
* EVILNUM (malware)
* Metamorfo (malware)
* Spica (malware)
* Trojan.Karagany (malware)
* Bandook (malware)
* PipeMon (malware)
* T9000 (malware)
* gh0st RAT (malware)
* Shamoon (malware)
* BLUELIGHT (malware)
* Kerrdown (malware)
* BPFDoor (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* OopsIE (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* Crutch (malware)
* SDBbot (malware)
* RTM (malware)
* SodaMaster (malware)
* Hikit (malware)
* StrelaStealer (malware)
* Grandoreiro (malware)
* Sakula (malware)
* GoBear (malware)
* Drovorub (malware)
* Bazar (malware)
* Kobalos (malware)
* XLoader (malware)
* Ryuk (malware)
* HermeticWiper (malware)
* Final1stspy (malware)
* MgBot (malware)
* Pandora (malware)
* FinFisher (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Wingbird (malware)
* Valak (malware)
* Samurai (malware)
* PoisonIvy (malware)
* NanoCore (malware)
* TajMahal (malware)
* Raccoon Stealer (malware)
* Daserf (malware)
* Carbon (malware)
* Pisloader (malware)
* Ramsay (malware)
* Pillowmint (malware)
* MacMa (malware)
* ROADSWEEP (malware)
* SUNSPOT (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* BackConfig (malware)
* PowGoop (malware)
* Nerex (malware)
* BoomBox (malware)
* PUNCHTRACK (malware)
* InnaputRAT (malware)
* GrimAgent (malware)
* LookBack (malware)
* Clop (malware)
* Lokibot (malware)
* Egregor (malware)
* PoetRAT (malware)
* CoinTicker (malware)
* Melcoz (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Maze (malware)
* ComRAT (malware)
* ChChes (malware)
* PowerStallion (malware)
* JPIN (malware)
* metaMain (malware)
* HTTPBrowser (malware)
* XCSSET (malware)
* KillDisk (malware)
* AppleJeus (malware)
* SoreFang (malware)
* MirageFox (malware)
* Industroyer (malware)
* Pcexter (malware)
* Agent Tesla (malware)
* ECCENTRICBANDWAGON (malware)
* BADNEWS (malware)
* Goopy (malware)
* ShadowPad (malware)
* Astaroth (malware)
* QakBot (malware)
* CookieMiner (malware)
* Hancitor (malware)
* Gelsemium (malware)
* jRAT (malware)
* Helminth (malware)
* Dridex (malware)
* Denis (malware)
* Waterbear (malware)
* Comnie (malware)
* H1N1 (malware)
* SLOWPULSE (malware)
* ADVSTORESHELL (malware)
* HiddenWasp (malware)
* Small Sieve (malware)
* HermeticWizard (malware)
* ShimRatReporter (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Empire (tool)
* PcShare (tool)
* CSPY Downloader (tool)
* CARROTBALL (tool)
* Brute Ratel C4 (tool)
* Remcos (tool)
* Out1 (tool)
* Imminent Monitor (tool)
* MCMD (tool)
* QuasarRAT (tool)
* LuminousMoth (intrusion-set)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* APT41 DUST (campaign)
* ArcaneDoor (campaign)
* OilRig (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* BlackTech (intrusion-set)
* APT42 (intrusion-set)
* Earth Lusca (intrusion-set)
* Operation CuckooBees (campaign)
* Sandworm Team (intrusion-set)
* Suckfly (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* Patchwork (intrusion-set)
* Cinnamon Tempest (intrusion-set)
* Darkhotel (intrusion-set)
* Ke3chang (intrusion-set)
* Operation Honeybee (campaign)
* 2016 Ukraine Electric Power Attack (campaign)
* MuddyWater (intrusion-set)
* APT38 (intrusion-set)
* APT32 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* BackdoorDiplomacy (intrusion-set)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* Storm-1811 (intrusion-set)
* Mustang Panda (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* Chimera (intrusion-set)
* RTM (intrusion-set)
* menuPass (intrusion-set)
* Tropic Trooper (intrusion-set)
* APT19 (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* Rocke (intrusion-set)
* Saint Bear (intrusion-set)
* Scattered Spider (intrusion-set)
* RedCurl (intrusion-set)
* Sidewinder (intrusion-set)
* Higaisa (intrusion-set)
* Windshift (intrusion-set)
* Threat Group-3390 (intrusion-set)
* Tonto Team (intrusion-set)
* Gamaredon Group (intrusion-set)
* Sea Turtle (intrusion-set)
* Moonstone Sleet (intrusion-set)
* APT3 (intrusion-set)
* Naikon (intrusion-set)
* C0017 (campaign)
* SideCopy (intrusion-set)
* Lotus Blossom (intrusion-set)
* Evilnum (intrusion-set)
* Whitefly (intrusion-set)
* APT-C-36 (intrusion-set)
* Gallmaker (intrusion-set)
* CopyKittens (intrusion-set)
* Star Blizzard (intrusion-set)
* PROMETHIUM (intrusion-set)
* BlackOasis (intrusion-set)

## Affected Products

* cpe:2.3:a:pypa:pipenv:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:34:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:35:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:36:\*:\*:\*:\*:\*:\*:\*