# CVE Detail – CVE-2022-29238

Jupyter Notebook is a web-based notebook environment for interactive computing. Prior to version 6.4.12, authenticated requests to the notebook server with `ContentsManager.allow\_hidden = False` only prevented listing the contents of hidden directories, not accessing individual hidden files or files in hidden directories (i.e. hidden files were 'hidden' but not 'inaccessible'). This could lead to notebook configurations allowing authenticated access to files that may reasonably be expected to be disallowed. Because fully authenticated requests are required, this is of relatively low impact. But if a server's root directory contains sensitive files whose only protection from the server is being hidden (e.g. `~/.ssh` while serving $HOME), then any authenticated requests could access files if their names are guessable. Such contexts also necessarily have full access to the server and therefore execution permissions, which also generally grants access to all the same files. So this does not generally result in any privilege escalation or increase in information access, only an additional, unintended means by which the files could be accessed. Version 6.4.12 contains a patch for this issue. There are currently no known workarounds.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.47628

## CVSS Scoring

CVSS v3.1 Score: 4.3

Severity: MEDIUM

## Mapped CWE(s)

* CWE-425: Direct Request ('Forced Browsing')

## CAPEC(s)

* CAPEC-127: Directory Indexing
* CAPEC-143: Detect Unpublicized Web Pages
* CAPEC-144: Detect Unpublicized Web Services
* CAPEC-668: Key Negotiation of Bluetooth Attack (KNOB)
* CAPEC-87: Forceful Browsing

## ATT&CK Techniques

* T1083: File and Directory Discovery
* T1565.002: Transmitted Data Manipulation

## Used By (Actors/Tools)

* TrickBot (malware)
* PowerDuke (malware)
* BLINDINGCAN (malware)
* Ninja (malware)
* QuietSieve (malware)
* SynAck (malware)
* AcidRain (malware)
* Amadey (malware)
* Proxysvc (malware)
* Orz (malware)
* yty (malware)
* Backdoor.Oldrea (malware)
* Stuxnet (malware)
* AvosLocker (malware)
* POWRUNER (malware)
* COATHANGER (malware)
* Smoke Loader (malware)
* WindTail (malware)
* Misdat (malware)
* KEYMARBLE (malware)
* ThreatNeedle (malware)
* RansomHub (malware)
* ZLib (malware)
* RedLeaves (malware)
* LITTLELAMB.WOOLTEA (malware)
* Zeus Panda (malware)
* GeminiDuke (malware)
* GravityRAT (malware)
* Prestige (malware)
* Bankshot (malware)
* SharpDisco (malware)
* StrongPity (malware)
* WinMM (malware)
* Nebulae (malware)
* AuditCred (malware)
* Kasidet (malware)
* OceanSalt (malware)
* Playcrypt (malware)
* Brave Prince (malware)
* RainyDay (malware)
* AppleSeed (malware)
* NETWIRE (malware)
* CosmicDuke (malware)
* Gomir (malware)
* Aria-body (malware)
* BOLDMOVE (malware)
* Crimson (malware)
* DUSTTRAP (malware)
* Turian (malware)
* Machete (malware)
* Action RAT (malware)
* Avenger (malware)
* Prikormka (malware)
* PingPull (malware)
* Dacls (malware)
* DropBook (malware)
* Woody RAT (malware)
* Mafalda (malware)
* ELMER (malware)
* SombRAT (malware)
* ODAgent (malware)
* FLASHFLOOD (malware)
* FYAnti (malware)
* LoFiSe (malware)
* HOPLIGHT (malware)
* Cuckoo Stealer (malware)
* MobileOrder (malware)
* WastedLocker (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* Volgmer (malware)
* WINERACK (malware)
* WhisperGate (malware)
* FruitFly (malware)
* AcidPour (malware)
* Skidmap (malware)
* Okrum (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Mispadu (malware)
* Megazord (malware)
* Diavol (malware)
* Doki (malware)
* Siloscape (malware)
* BlackCat (malware)
* Fysbis (malware)
* MarkiRAT (malware)
* Kazuar (malware)
* NETEAGLE (malware)
* POORAIM (malware)
* CHIMNEYSWEEP (malware)
* FatDuke (malware)
* BlackEnergy (malware)
* zwShell (malware)
* Rising Sun (malware)
* NotPetya (malware)
* ShimRat (malware)
* BADFLICK (malware)
* ObliqueRAT (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* XAgentOSX (malware)
* China Chopper (malware)
* LightSpy (malware)
* Cheerscrypt (malware)
* KeyBoy (malware)
* MiniDuke (malware)
* Pteranodon (malware)
* ROKRAT (malware)
* Babuk (malware)
* Exbyte (malware)
* DarkWatchman (malware)
* BlackMould (malware)
* PACEMAKER (malware)
* BBSRAT (malware)
* PlugX (malware)
* Bisonal (malware)
* MultiLayer Wiper (malware)
* DustySky (malware)
* Remsec (malware)
* Rover (malware)
* Epic (malware)
* LightNeuron (malware)
* Peppy (malware)
* Cuba (malware)
* DEATHRANSOM (malware)
* Clambling (malware)
* Akira (malware)
* DarkGate (malware)
* LockBit 3.0 (malware)
* FoggyWeb (malware)
* Hydraq (malware)
* CreepyDrive (malware)
* Caterpillar WebShell (malware)
* Elise (malware)
* USBferry (malware)
* WannaCry (malware)
* TSCookie (malware)
* Latrodectus (malware)
* Saint Bot (malware)
* CharmPower (malware)
* TYPEFRAME (malware)
* 3PARA RAT (malware)
* TAINTEDSCRIBE (malware)
* Royal (malware)
* Uroburos (malware)
* Metamorfo (malware)
* Spica (malware)
* Trojan.Karagany (malware)
* Bandook (malware)
* TINYTYPHON (malware)
* KONNI (malware)
* CORALDECK (malware)
* SPACESHIP (malware)
* BLUELIGHT (malware)
* KGH\_SPY (malware)
* down\_new (malware)
* Ixeshe (malware)
* Micropsia (malware)
* RARSTONE (malware)
* Black Basta (malware)
* 4H RAT (malware)
* Attor (malware)
* MegaCortex (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* Akira \_v2 (malware)
* SDBbot (malware)
* RTM (malware)
* Derusbi (malware)
* Bazar (malware)
* BadPatch (malware)
* MESSAGETAP (malware)
* SUGARDUMP (malware)
* SOUNDBITE (malware)
* MoonWind (malware)
* Ryuk (malware)
* Cryptoistic (malware)
* HermeticWiper (malware)
* ccf32 (malware)
* LockBit 2.0 (malware)
* Zebrocy (malware)
* FinFisher (malware)
* LunarMail (malware)
* CrossRAT (malware)
* OwaAuth (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* HotCroissant (malware)
* REvil (malware)
* Samurai (malware)
* PinchDuke (malware)
* USBStealer (malware)
* Taidoor (malware)
* Kivars (malware)
* CaddyWiper (malware)
* Cyclops Blink (malware)
* Seasalt (malware)
* TajMahal (malware)
* PLEAD (malware)
* Raccoon Stealer (malware)
* Cardinal RAT (malware)
* Pisloader (malware)
* GoldenSpy (malware)
* Gold Dragon (malware)
* Ramsay (malware)
* MacMa (malware)
* FunnyDream (malware)
* ROADSWEEP (malware)
* SUNSPOT (malware)
* SysUpdate (malware)
* OutSteel (malware)
* BackConfig (malware)
* Kwampirs (malware)
* BoomBox (malware)
* Mango (malware)
* InnaputRAT (malware)
* GrimAgent (malware)
* LookBack (malware)
* Clop (malware)
* Lokibot (malware)
* PoetRAT (malware)
* CHOPSTICK (malware)
* StealBit (malware)
* ZxShell (malware)
* NDiskMonitor (malware)
* DDKONG (malware)
* Penquin (malware)
* BabyShark (malware)
* Cannon (malware)
* Melcoz (malware)
* Winnti for Windows (malware)
* Troll Stealer (malware)
* BLACKCOFFEE (malware)
* Kinsing (malware)
* njRAT (malware)
* ZIPLINE (malware)
* ChChes (malware)
* Manjusaka (malware)
* IceApple (malware)
* JPIN (malware)
* metaMain (malware)
* SideTwist (malware)
* Psylo (malware)
* Heyoka Backdoor (malware)
* HTTPBrowser (malware)
* LunarWeb (malware)
* XCSSET (malware)
* Octopus (malware)
* KillDisk (malware)
* SoreFang (malware)
* Industroyer (malware)
* Pcexter (malware)
* Pasam (malware)
* BADNEWS (malware)
* Linfo (malware)
* Remexi (malware)
* QakBot (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* jRAT (malware)
* OSX/Shlayer (malware)
* Denis (malware)
* INC Ransomware (malware)
* FIVEHANDS (malware)
* AutoIt backdoor (malware)
* Dtrack (malware)
* Azorult (malware)
* BACKSPACE (malware)
* Zox (malware)
* UPPERCUT (malware)
* ADVSTORESHELL (malware)
* StrifeWater (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* FALLCHILL (malware)
* RemoteUtilities (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* Empire (tool)
* PoshC2 (tool)
* Rclone (tool)
* Remcos (tool)
* Imminent Monitor (tool)
* Forfiles (tool)
* cmd (tool)
* CrackMapExec (tool)
* Koadic (tool)
* Pupy (tool)
* LuminousMoth (intrusion-set)
* Operation Wocao (campaign)
* Velvet Ant (intrusion-set)
* Dragonfly (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Inception (intrusion-set)
* admin@338 (intrusion-set)
* Operation CuckooBees (campaign)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Turla (intrusion-set)
* TeamTNT (intrusion-set)
* Patchwork (intrusion-set)
* APT28 (intrusion-set)
* Aoqin Dragon (intrusion-set)
* Darkhotel (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* Operation Honeybee (campaign)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* MuddyWater (intrusion-set)
* APT38 (intrusion-set)
* APT32 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* APT5 (intrusion-set)
* Kimsuky (intrusion-set)
* Mustang Panda (intrusion-set)
* Chimera (intrusion-set)
* ToddyCat (intrusion-set)
* menuPass (intrusion-set)
* Tropic Trooper (intrusion-set)
* Operation Dream Job (campaign)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* Scattered Spider (intrusion-set)
* Windigo (intrusion-set)
* RedCurl (intrusion-set)
* Sidewinder (intrusion-set)
* Confucius (intrusion-set)
* Gamaredon Group (intrusion-set)
* Night Dragon (campaign)
* Dark Caracal (intrusion-set)
* APT3 (intrusion-set)
* Sowbug (intrusion-set)
* Winter Vivern (intrusion-set)
* Lotus Blossom (intrusion-set)
* APT18 (intrusion-set)
* KV Botnet Activity (campaign)

## Affected Products

* cpe:2.3:a:jupyter:notebook:\*:\*:\*:\*:\*:\*:\*:\*