# CVE Detail – CVE-2009-3489

Adobe Photoshop Elements 8.0 installs the Adobe Active File Monitor V8 service with an insecure security descriptor, which allows local users to (1) stop the service via the stop command, (2) execute arbitrary commands as SYSTEM by using the config command to modify the binPath variable, or (3) restart the service via the start command.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.45888

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-732: Incorrect Permission Assignment for Critical Resource

## CAPEC(s)

* CAPEC-1: Accessing Functionality Not Properly Constrained by ACLs
* CAPEC-122: Privilege Abuse
* CAPEC-127: Directory Indexing
* CAPEC-17: Using Malicious Files
* CAPEC-180: Exploiting Incorrectly Configured Access Control Security Levels
* CAPEC-206: Signing Malicious Code
* CAPEC-234: Hijacking a privileged process
* CAPEC-60: Reusing Session IDs (aka Session Replay)
* CAPEC-61: Session Fixation
* CAPEC-62: Cross Site Request Forgery
* CAPEC-642: Replace Binaries

## ATT&CK Techniques

* T1553.002: Code Signing
* T1505.005: Terminal Services DLL
* T1548: Abuse Elevation Control Mechanism
* T1574.005: Executable Installer File Permissions Weakness
* T1083: File and Directory Discovery
* T1134.001: Token Impersonation/Theft
* T1554: Compromise Host Software Binary
* T1574.010: Services File Permissions Weakness
* T1550.004: Web Session Cookie

## 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)
* Janicab (malware)
* AuditCred (malware)
* Kasidet (malware)
* OceanSalt (malware)
* Playcrypt (malware)
* Brave Prince (malware)
* RainyDay (malware)
* Ecipekac (malware)
* AppleSeed (malware)
* BUSHWALK (malware)
* NETWIRE (malware)
* CosmicDuke (malware)
* GreyEnergy (malware)
* Gomir (malware)
* Aria-body (malware)
* Emotet (malware)
* BOLDMOVE (malware)
* Crimson (malware)
* DUSTTRAP (malware)
* Turian (malware)
* BADHATCH (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)
* Bonadan (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)
* BOOSTWRITE (malware)
* Rising Sun (malware)
* NotPetya (malware)
* ShimRat (malware)
* BADFLICK (malware)
* ObliqueRAT (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* SpicyOmelette (malware)
* XAgentOSX (malware)
* China Chopper (malware)
* LockerGoga (malware)
* LightSpy (malware)
* Cheerscrypt (malware)
* LIGHTWIRE (malware)
* KeyBoy (malware)
* MiniDuke (malware)
* Anchor (malware)
* Pteranodon (malware)
* ROKRAT (malware)
* Babuk (malware)
* Exbyte (malware)
* DarkWatchman (malware)
* BlackMould (malware)
* PACEMAKER (malware)
* BBSRAT (malware)
* PlugX (malware)
* Bisonal (malware)
* MultiLayer Wiper (malware)
* Lumma Stealer (malware)
* DustySky (malware)
* Remsec (malware)
* Rover (malware)
* Epic (malware)
* Peppy (malware)
* Cuba (malware)
* DEATHRANSOM (malware)
* Clambling (malware)
* Akira (malware)
* DarkGate (malware)
* LockBit 3.0 (malware)
* ThiefQuest (malware)
* FoggyWeb (malware)
* Hydraq (malware)
* CreepyDrive (malware)
* Caterpillar WebShell (malware)
* Elise (malware)
* USBferry (malware)
* WannaCry (malware)
* Gazer (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)
* PipeMon (malware)
* TINYTYPHON (malware)
* KONNI (malware)
* Shamoon (malware)
* CORALDECK (malware)
* SPACESHIP (malware)
* BLUELIGHT (malware)
* KGH\_SPY (malware)
* down\_new (malware)
* Ixeshe (malware)
* Micropsia (malware)
* RARSTONE (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* 4H RAT (malware)
* Attor (malware)
* MegaCortex (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* Akira \_v2 (malware)
* SDBbot (malware)
* RTM (malware)
* Derusbi (malware)
* StrelaStealer (malware)
* Tarrask (malware)
* GoBear (malware)
* Bazar (malware)
* Kobalos (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)
* WARPWIRE (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)
* Daserf (malware)
* Cardinal RAT (malware)
* Pisloader (malware)
* GoldenSpy (malware)
* Gold Dragon (malware)
* Ramsay (malware)
* FRAMESTING (malware)
* MacMa (malware)
* FunnyDream (malware)
* ROADSWEEP (malware)
* SUNSPOT (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* OutSteel (malware)
* BackConfig (malware)
* Kwampirs (malware)
* Nerex (malware)
* BoomBox (malware)
* Mango (malware)
* InnaputRAT (malware)
* WIREFIRE (malware)
* Kessel (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)
* Winnti for Windows (malware)
* Troll Stealer (malware)
* BLACKCOFFEE (malware)
* BFG Agonizer (malware)
* Ebury (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)
* AppleJeus (malware)
* SoreFang (malware)
* Industroyer (malware)
* Pcexter (malware)
* Pasam (malware)
* BADNEWS (malware)
* Linfo (malware)
* Remexi (malware)
* QakBot (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* jRAT (malware)
* Helminth (malware)
* OSX/Shlayer (malware)
* Denis (malware)
* INC Ransomware (malware)
* FIVEHANDS (malware)
* AutoIt backdoor (malware)
* Dtrack (malware)
* SLOWPULSE (malware)
* Azorult (malware)
* BitPaymer (malware)
* BACKSPACE (malware)
* Zox (malware)
* UPPERCUT (malware)
* ADVSTORESHELL (malware)
* StrifeWater (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* FALLCHILL (malware)
* HermeticWizard (malware)
* RemoteUtilities (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* Empire (tool)
* PoshC2 (tool)
* CSPY Downloader (tool)
* Rclone (tool)
* Remcos (tool)
* Imminent Monitor (tool)
* Forfiles (tool)
* cmd (tool)
* CrackMapExec (tool)
* Koadic (tool)
* Pupy (tool)
* QuasarRAT (tool)
* LuminousMoth (intrusion-set)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* APT41 DUST (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* Inception (intrusion-set)
* admin@338 (intrusion-set)
* Operation CuckooBees (campaign)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Turla (intrusion-set)
* Suckfly (intrusion-set)
* TeamTNT (intrusion-set)
* FIN6 (intrusion-set)
* Silence (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)
* 2016 Ukraine Electric Power Attack (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)
* Leviathan (intrusion-set)
* Mustang Panda (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* Chimera (intrusion-set)
* ToddyCat (intrusion-set)
* menuPass (intrusion-set)
* Tropic Trooper (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* FIN8 (intrusion-set)
* Saint Bear (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)
* HomeLand Justice (campaign)
* Winter Vivern (intrusion-set)
* Cutting Edge (campaign)
* Lotus Blossom (intrusion-set)
* APT18 (intrusion-set)
* KV Botnet Activity (campaign)
* CopyKittens (intrusion-set)
* Star Blizzard (intrusion-set)
* PROMETHIUM (intrusion-set)

## Affected Products

* cpe:2.3:a:adobe:photoshop\_elements:8.0:\*:\*:\*:\*:\*:\*:\*