# CVE Detail – CVE-2020-10148

The SolarWinds Orion API is vulnerable to an authentication bypass that could allow a remote attacker to execute API commands. This vulnerability could allow a remote attacker to bypass authentication and execute API commands which may result in a compromise of the SolarWinds instance. SolarWinds Orion Platform versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1 are affected.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.99948

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-288: Authentication Bypass Using an Alternate Path or Channel
* CWE-306: Missing Authentication for Critical Function

## CAPEC(s)

* CAPEC-12: Choosing Message Identifier
* CAPEC-127: Directory Indexing
* CAPEC-166: Force the System to Reset Values
* CAPEC-216: Communication Channel Manipulation
* CAPEC-36: Using Unpublished Interfaces or Functionality
* CAPEC-62: Cross Site Request Forgery
* CAPEC-665: Exploitation of Thunderbolt Protection Flaws

## ATT&CK Techniques

* T1542.002: Component Firmware
* T1083: File and Directory Discovery
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## 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)
* 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)
* 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)
* 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)
* 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)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* Equation (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:solarwinds:orion\_platform:2019.4:hotfix5:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:solarwinds:orion\_platform:2020.2:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:solarwinds:orion\_platform:2020.2.1:hotfix1:\*:\*:\*:\*:\*:\*