# CVE Detail – CVE-2022-24765

Git for Windows is a fork of Git containing Windows-specific patches. This vulnerability affects users working on multi-user machines, where untrusted parties have write access to the same hard disk. Those untrusted parties could create the folder `C:\.git`, which would be picked up by Git operations run supposedly outside a repository while searching for a Git directory. Git would then respect any config in said Git directory. Git Bash users who set `GIT\_PS1\_SHOWDIRTYSTATE` are vulnerable as well. Users who installed posh-gitare vulnerable simply by starting a PowerShell. Users of IDEs such as Visual Studio are vulnerable: simply creating a new project would already read and respect the config specified in `C:\.git\config`. Users of the Microsoft fork of Git are vulnerable simply by starting a Git Bash. The problem has been patched in Git for Windows v2.35.2. Users unable to upgrade may create the folder `.git` on all drives where Git commands are run, and remove read/write access from those folders as a workaround. Alternatively, define or extend `GIT\_CEILING\_DIRECTORIES` to cover the \_parent\_ directory of the user profile, e.g. `C:\Users` if the user profile is located in `C:\Users\my-user-name`.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.38871

## CVSS Scoring

CVSS v3.1 Score: 6.0

Severity: MEDIUM

## Mapped CWE(s)

* CWE-427: Uncontrolled Search Path Element

## CAPEC(s)

* CAPEC-38: Leveraging/Manipulating Configuration File Search Paths
* CAPEC-471: Search Order Hijacking

## ATT&CK Techniques

* T1574.007: Path Interception by PATH Environment Variable
* T1574.001: DLL
* T1574.008: Path Interception by Search Order Hijacking
* T1574.009: Path Interception by Unquoted Path
* T1574.004: Dylib Hijacking

## Used By (Actors/Tools)

* Ninja (malware)
* RCSession (malware)
* Downdelph (malware)
* Chinoxy (malware)
* RedLeaves (malware)
* WEBC2 (malware)
* Nebulae (malware)
* RainyDay (malware)
* Ecipekac (malware)
* Prikormka (malware)
* LoFiSe (malware)
* WastedLocker (malware)
* InvisiMole (malware)
* ZeroT (malware)
* Raspberry Robin (malware)
* HUI Loader (malware)
* BOOSTWRITE (malware)
* HyperBro (malware)
* Javali (malware)
* BBSRAT (malware)
* PlugX (malware)
* Lumma Stealer (malware)
* Clambling (malware)
* DarkGate (malware)
* FoggyWeb (malware)
* Chaes (malware)
* Metamorfo (malware)
* T9000 (malware)
* gh0st RAT (malware)
* Kerrdown (malware)
* Crutch (malware)
* Hikit (malware)
* StrelaStealer (malware)
* Sakula (malware)
* Pandora (malware)
* FinFisher (malware)
* Wingbird (malware)
* Ramsay (malware)
* SysUpdate (malware)
* PowGoop (malware)
* LookBack (malware)
* Egregor (malware)
* Melcoz (malware)
* metaMain (malware)
* HTTPBrowser (malware)
* MirageFox (malware)
* Pcexter (malware)
* BADNEWS (malware)
* Goopy (malware)
* Astaroth (malware)
* QakBot (malware)
* Dridex (malware)
* Denis (malware)
* Waterbear (malware)
* PowerSploit (tool)
* Empire (tool)
* Brute Ratel C4 (tool)
* LuminousMoth (intrusion-set)
* Velvet Ant (intrusion-set)
* APT41 DUST (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Daggerfly (intrusion-set)
* BlackTech (intrusion-set)
* Earth Lusca (intrusion-set)
* Operation CuckooBees (campaign)
* Patchwork (intrusion-set)
* Cinnamon Tempest (intrusion-set)
* MuddyWater (intrusion-set)
* APT32 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* BackdoorDiplomacy (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)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* Sidewinder (intrusion-set)
* Higaisa (intrusion-set)
* Threat Group-3390 (intrusion-set)
* Tonto Team (intrusion-set)
* APT3 (intrusion-set)
* Naikon (intrusion-set)
* SideCopy (intrusion-set)
* Evilnum (intrusion-set)
* Whitefly (intrusion-set)

## Affected Products

* cpe:2.3:a:git-scm:git:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:34:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:35:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:36:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:37:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apple:xcode:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*