# CVE Detail – CVE-2004-0030

PHP remote file inclusion vulnerability in (1) functions.php, (2) authentication\_index.php, and (3) config\_gedcom.php for PHPGEDVIEW 2.61 allows remote attackers to execute arbitrary PHP code by modifying the PGV\_BASE\_DIRECTORY parameter to reference a URL on a remote web server that contains the code.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.9111

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-829: Inclusion of Functionality from Untrusted Control Sphere

## CAPEC(s)

* CAPEC-175: Code Inclusion
* CAPEC-201: Serialized Data External Linking
* CAPEC-228: DTD Injection
* CAPEC-251: Local Code Inclusion
* CAPEC-252: PHP Local File Inclusion
* CAPEC-253: Remote Code Inclusion
* CAPEC-263: Force Use of Corrupted Files
* CAPEC-538: Open-Source Library Manipulation
* CAPEC-549: Local Execution of Code
* CAPEC-640: Inclusion of Code in Existing Process
* CAPEC-660: Root/Jailbreak Detection Evasion via Hooking
* CAPEC-695: Repo Jacking
* CAPEC-698: Install Malicious Extension

## ATT&CK Techniques

* T1195.001: Compromise Software Dependencies and Development Tools
* T1505.005: Terminal Services DLL
* T1176: Software Extensions
* T1055: Process Injection
* T1620: Reflective Code Loading
* T1574.006: Dynamic Linker Hijacking
* T1574.013: KernelCallbackTable
* T1505.004: IIS Components

## Used By (Actors/Tools)

* TrickBot (malware)
* Ninja (malware)
* Pikabot (malware)
* Wiarp (malware)
* Bumblebee (malware)
* Backdoor.Oldrea (malware)
* COATHANGER (malware)
* Sardonic (malware)
* Smoke Loader (malware)
* AuditCred (malware)
* NETWIRE (malware)
* Emotet (malware)
* DUSTTRAP (malware)
* BADHATCH (malware)
* Avenger (malware)
* Woody RAT (malware)
* Hildegard (malware)
* BlackByte 2.0 Ransomware (malware)
* HOPLIGHT (malware)
* GuLoader (malware)
* InvisiMole (malware)
* WhisperGate (malware)
* Mispadu (malware)
* NavRAT (malware)
* CostaBricks (malware)
* HyperBro (malware)
* ROKRAT (malware)
* Dyre (malware)
* LunarLoader (malware)
* Lumma Stealer (malware)
* Cuba (malware)
* Clambling (malware)
* ThiefQuest (malware)
* FoggyWeb (malware)
* Gazer (malware)
* TSCookie (malware)
* Uroburos (malware)
* gh0st RAT (malware)
* JHUHUGIT (malware)
* StoneDrill (malware)
* Attor (malware)
* Bazar (malware)
* Ryuk (malware)
* ABK (malware)
* Pandora (malware)
* FinFisher (malware)
* OwaAuth (malware)
* Cobalt Strike (malware)
* Wingbird (malware)
* REvil (malware)
* Cardinal RAT (malware)
* RGDoor (malware)
* Lokibot (malware)
* Egregor (malware)
* Ebury (malware)
* ANDROMEDA (malware)
* IceApple (malware)
* JPIN (malware)
* metaMain (malware)
* Mis-Type (malware)
* XCSSET (malware)
* Agent Tesla (malware)
* ShadowPad (malware)
* QakBot (malware)
* Gelsemium (malware)
* BBK (malware)
* Waterbear (malware)
* Lizar (malware)
* HiddenWasp (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Empire (tool)
* PcShare (tool)
* PoshC2 (tool)
* Brute Ratel C4 (tool)
* Remcos (tool)
* Donut (tool)
* IronNetInjector (tool)
* HTRAN (tool)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Turla (intrusion-set)
* Silence (intrusion-set)
* Cobalt Group (intrusion-set)
* APT38 (intrusion-set)
* APT32 (intrusion-set)
* APT5 (intrusion-set)
* Kimsuky (intrusion-set)
* TA2541 (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* Operation Dream Job (campaign)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* PLATINUM (intrusion-set)
* Rocke (intrusion-set)
* BlackByte (intrusion-set)
* Operation Sharpshooter (campaign)
* Cutting Edge (campaign)

## Affected Products

* cpe:2.3:a:phpgedview:phpgedview:2.61:\*:\*:\*:\*:\*:\*:\*