# CVE Detail – CVE-2005-1111

Race condition in cpio 2.6 and earlier allows local users to modify permissions of arbitrary files via a hard link attack on a file while it is being decompressed, whose permissions are changed by cpio after the decompression is complete.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.23234

## CVSS Scoring

CVSS v3.1 Score: 4.7

Severity: MEDIUM

## Mapped CWE(s)

* CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition
* CWE-59: Improper Link Resolution Before File Access ('Link Following')

## CAPEC(s)

* CAPEC-132: Symlink Attack
* CAPEC-17: Using Malicious Files
* CAPEC-27: Leveraging Race Conditions via Symbolic Links
* CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
* CAPEC-35: Leverage Executable Code in Non-Executable Files
* CAPEC-76: Manipulating Web Input to File System Calls

## ATT&CK Techniques

* T1027.009: Embedded Payloads
* T1547.009: Shortcut Modification
* T1574.005: Executable Installer File Permissions Weakness
* T1574.010: Services File Permissions Weakness
* T1564.009: Resource Forking
* T1027.006: HTML Smuggling

## Used By (Actors/Tools)

* Pikabot (malware)
* RedLeaves (malware)
* macOS.OSAMiner (malware)
* EnvyScout (malware)
* SslMM (malware)
* Emotet (malware)
* DUSTTRAP (malware)
* BADHATCH (malware)
* DUSTPAN (malware)
* Moneybird (malware)
* InvisiMole (malware)
* Keydnap (malware)
* Okrum (malware)
* IcedID (malware)
* MarkiRAT (malware)
* Kazuar (malware)
* CHIMNEYSWEEP (malware)
* BlackEnergy (malware)
* Reaver (malware)
* MultiLayer Wiper (malware)
* S-Type (malware)
* SeaDuke (malware)
* Netwalker (malware)
* Gazer (malware)
* SMOKEDHAM (malware)
* Uroburos (malware)
* KONNI (malware)
* SPACESHIP (malware)
* Micropsia (malware)
* RogueRobin (malware)
* Grandoreiro (malware)
* Bazar (malware)
* SHIPSHAPE (malware)
* TinyZBot (malware)
* DEADEYE (malware)
* FELIXROOT (malware)
* ComRAT (malware)
* Astaroth (malware)
* QakBot (malware)
* Helminth (malware)
* OSX/Shlayer (malware)
* DEADWOOD (malware)
* Comnie (malware)
* Dtrack (malware)
* BACKSPACE (malware)
* Empire (tool)
* Invoke-PSImage (tool)
* Lazarus Group (intrusion-set)
* TA577 (intrusion-set)
* APT29 (intrusion-set)
* APT39 (intrusion-set)
* Leviathan (intrusion-set)
* Gorgon Group (intrusion-set)
* C0021 (campaign)
* Moonstone Sleet (intrusion-set)

## Affected Products

* cpe:2.3:a:gnu:cpio:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:3.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:4.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:5.04:\*:\*:\*:\*:\*:\*:\*