# CVE Detail – CVE-2020-26277

DBdeployer is a tool that deploys MySQL database servers easily. In DBdeployer before version 1.58.2, users unpacking a tarball may use a maliciously packaged tarball that contains symlinks to files external to the target. In such scenario, an attacker could induce dbdeployer to write into a system file, thus altering the computer defenses. For the attack to succeed, the following factors need to contribute: 1) The user is logged in as root. While dbdeployer is usable as root, it was designed to run as unprivileged user. 2) The user has taken a tarball from a non secure source, without testing the checksum. When the tarball is retrieved through dbdeployer, the checksum is compared before attempting to unpack. This has been fixed in version 1.58.2.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.53209

## CVSS Scoring

CVSS v3.1 Score: 6.1

Severity: MEDIUM

## Mapped CWE(s)

* CWE-59: Improper Link Resolution Before File Access ('Link Following')

## CAPEC(s)

* CAPEC-132: Symlink Attack
* CAPEC-17: Using Malicious Files
* 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:dbdeployer:dbdeployer:\*:\*:\*:\*:\*:\*:\*:\*