# CVE Detail – CVE-2007-5626

make\_catalog\_backup in Bacula 2.2.5, and probably earlier, sends a MySQL password as a command line argument, and sometimes transmits cleartext e-mail containing this command line, which allows context-dependent attackers to obtain the password by listing the process and its arguments, or by sniffing the network.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.08

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-319: Cleartext Transmission of Sensitive Information

## CAPEC(s)

* CAPEC-102: Session Sidejacking
* CAPEC-117: Interception
* CAPEC-383: Harvesting Information via API Event Monitoring
* CAPEC-477: Signature Spoofing by Mixing Signed and Unsigned Content
* CAPEC-65: Sniff Application Code

## ATT&CK Techniques

* T1040: Network Sniffing
* T1056.004: Credential API Hooking

## Used By (Actors/Tools)

* TrickBot (malware)
* cd00r (malware)
* JumbledPath (malware)
* RDFSNIFFER (malware)
* NOKKI (malware)
* VersaMem (malware)
* Ursnif (malware)
* Zeus Panda (malware)
* J-magic (malware)
* Emotet (malware)
* Regin (malware)
* Line Dancer (malware)
* FoggyWeb (malware)
* MESSAGETAP (malware)
* Zebrocy (malware)
* FinFisher (malware)
* Carberp (malware)
* ZxShell (malware)
* Penquin (malware)
* Impacket (tool)
* Empire (tool)
* PoshC2 (tool)
* Responder (tool)
* NBTscan (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Sandworm Team (intrusion-set)
* APT28 (intrusion-set)
* Kimsuky (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* DarkVishnya (intrusion-set)
* PLATINUM (intrusion-set)
* Salt Typhoon (intrusion-set)
* APT33 (intrusion-set)

## Affected Products

* cpe:2.3:a:bacula:bacula:\*:\*:\*:\*:\*:\*:\*:\*