# CVE Detail – CVE-2002-1872

Microsoft SQL Server 6.0 through 2000, with SQL Authentication enabled, uses weak password encryption (XOR), which allows remote attackers to sniff and decrypt the password.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.80802

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-326: Inadequate Encryption Strength

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-192: Protocol Analysis
* CAPEC-20: Encryption Brute Forcing

## ATT&CK Techniques

* T1110: Brute Force

## Used By (Actors/Tools)

* Chaos (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Kinsing (malware)
* QakBot (malware)
* PoshC2 (tool)
* CrackMapExec (tool)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:a:microsoft:sql\_server:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:6.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:7.0:sp1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:7.0:sp2:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:7.0:sp3:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:7.0:sp4:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:2000:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:2000:sp1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:microsoft:sql\_server:2000:sp2:\*:\*:\*:\*:\*:\*