# CVE Detail – CVE-2002-0969

Buffer overflow in MySQL daemon (mysqld) before 3.23.50, and 4.0 beta before 4.02, on the Win32 platform, allows local users to execute arbitrary code via a long "datadir" parameter in the my.ini initialization file, whose permissions on Windows allow Full Control to the Everyone group.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.29103

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-100: Overflow Buffers
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-42: MIME Conversion
* CAPEC-44: Overflow Binary Resource File
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-67: String Format Overflow in syslog()
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities
* CAPEC-92: Forced Integer Overflow

## Affected Products

* cpe:2.3:a:oracle:mysql:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:mysql:\*:\*:\*:\*:\*:\*:\*:\*