



CVE-2003-0073

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2003-0073
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-02-19 05:00:00 UTC
Updated	2019-10-07 16:41:00 UTC
Description	Double-free vulnerability in mysqld for MySQL before 3.23.55 allows attackers with MySQL access to cause a denial of service

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Mysql	3.23.31	All	All	All
Application	Oracle	Mysql	3.23.36	All	All	All
Application	Oracle	Mysql	3.23.41	All	All	All
Application	Oracle	Mysql	3.23.47	All	All	All
Application	Oracle	Mysql	3.23.52	All	All	All
Application	Oracle	Mysql	3.23.53	All	All	All
Application	Oracle	Mysql	3.23.54	All	All	All
Application	Oracle	Mysql	3.23.54a	All	All	All
Application	Oracle	Mysql	3.23.31	All	All	All
Application	Oracle	Mysql	3.23.36	All	All	All
Application	Oracle	Mysql	3.23.41	All	All	All
Application	Oracle	Mysql	3.23.47	All	All	All
Application	Oracle	Mysql	3.23.52	All	All	All
Application	Oracle	Mysql	3.23.53	All	All	All
Application	Oracle	Mysql	3.23.54	All	All	All
Application	Oracle	Mysql	3.23.54a	All	All	All

References
Reference
redhat.com Red Hat Support
Debian -- Security Information -- DSA-303-1 mysql
MySQL Double Free Heap Corruption Vulnerability
MySQL Manual D.4.5 Changes in release 3.23.55 (23 Jan 2003)
'[OpenPKG-SA-2003.008] OpenPKG Security Advisory (mysql)' - MARC
ISS X-Force Database:mysql-mysqlchangeuser-doublefree-dos(11199): MySQL mysql_change_user() double-free memory pointer denial of s
Home - Conectiva
LinuxSecurity.com: EnGarde: MySQL double free vulnerability
redhat.com Red Hat Support
redhat.com Red Hat Support
Mandrakesoft Security Advisories
Repository / Oval Repository
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.