

CVE-2020-13127

By [divzeronz](https://blog.divisionzero.co/author/divzeronz/) <<https://blog.divisionzero.co/author/divzeronz/>>



18th May 2020 <<https://blog.divisionzero.co/2020/05/18/cve-2020-13127/>>

A SQL injection vulnerability at `/queuemetrics/tpf` in Loway QueueMetrics before 19.04.1 allows remote authenticated attackers to execute arbitrary SQL commands via the `TASKS_LIST__pt.querystring` parameter.

The high severity issue was reported to the Vendor who implemented a fix. QueueMetrics users should upgrade to the latest available version.

```
11:35:00] [100] Fetching columns for table 'arch_users' in database 'queuemetrics'
Database: queuemetrics
Table: arch_users
(28 columns)
```

Column	Type
abilitato	tinyint(4)
chiavi_utente	text
classe	int(11)
commento	varchar(200)
email	varchar(50)
login	varchar(50)
masterkey	tinyint(4)
n_logon	int(11)
PASSWORD	varchar(200)
psalt	varchar(100)
pversion	int(11)
real_name	varchar(50)
sys_dt_crazione	datetime
sys_dt_modifica	datetime
sys_optlock	int(11)
sys_user_crazione	int(11)
sys_user_modifica	int(11)
token	varchar(50)
ultimo_logon	datetime
user_id	int(11)

Date Reported to Vendor: 16 June, 2019

Affected Application: QueueMetrics v18.04.1

Fixed Version: 19.10

Severity: High

CVSS: 8.1

[Advisories < https://blog.divisionzero.co/category/advisories/ >](https://blog.divisionzero.co/category/advisories/)

[Blog < https://blog.divisionzero.co/category/blog/ >](https://blog.divisionzero.co/category/blog/)