MySQL Dynamic SQL Injecti Monitor

BUG_Author: Chengxin Xu
Affected Version: frostmourne (1.0)
Vendor: frostmourne GitHub Repository
Software: frostmourne
Vulnerability Files:

- `frostmourne-monitor/src/main/java/com/autohome/frostmou qlDataQuery.java`
- `frostmourne-monitor/src/main/java/com/autohome/frostmou sqlObjectMetric.java`
- `frostmourne-monitor/src/main/java/com/autohome/frostmou java`

Description

Frostmourne Monitor contains a MySQL dynamic SQL injectio `metricContract.queryString` value is treated as trust queries without parameterization or whitelist validation. An au preview functionality can first enumerate an available MySQL expressions that are executed by the server against the corre

MySQL Dynamic SQL Injection via Alarm Prev

The vulnerability chain starts from the `AlarmController. api/alarm/previewData`. User-controlled JSON is accep implementation without sanitizing the supplied SQL string: