CVE-2018-3754 CWE-89 (SQL)

query-mysql

```
var mysql      = require('mysql');
module.exports = function () {
  var connection = null;

  function connect(callback) {
    connection.connect(function (err){
      if(!err) {
          callback(true)
      } else {
          callback(false);
      }
    });
  }

  [...]

  fetchById: function (table, id, name_id, callback) {
        connect(function (connected) {
          if (connected) {

            connection.query("SELECT * FROM " + table + " WHERE " +name_id+"='"+
id+"'", function (err, rows, fields) {
              connection.end();
              console.log("fetchById");
              //if (err) throw err;
              if (err) {
                callback("error", null);
              }else{
                callback("success", rows);
              };
            })

          }else{
            callback("error_connection", null);
          };
        })
      },
```

CVE-2018-16460

CWE-78 (OS cmd)

ps

```
var ps = require('ps');

ps.lookup({ pid: "$(touch success.txt)" }, function(err, proc) { // this method
is vulnerable to command injection
    if (err) {throw err;}
    if (proc) {
        console.log(proc);  // Process name, something like "node" or "bash"
    } else {
        console.log('No such process');
    }
});
```

CVE-2019-5413

CWE-77 (cmd)

Morgan

```
function morgan (format, options) {
  var fmt = format
  var opts = options || {}

  if (format && typeof format === 'object') {
    opts = format
    fmt = opts.format || 'default'

... (payload ex)
var morgan = require('morgan');
var f = morgan('25 \\" + console.log(\'hello!\'); +  //:method :url :status
:res[content-length] - :response-time ms');
f({}, {}, function () {
});
```