

20200309 Authenticated SQL injection

[Jump to bottom](#)

Arjen van Bochoven edited this page on Mar 9, 2020 · 1 revision

Authenticated SQL injection - CVE-2020-10190

Description

A logged in admin can craft a special request using his admin session credentials to inject arbitrary SQL into a webquery. This can lead to reading records outside of the authorization of the admin - for instance when using Business Units. Using this special request, it is also possible to alter and delete arbitrary records.

Vulnerability: All versions of MunkiReport < 5.3.0 are vulnerable

Mitigation

Update MunkiReport to the latest version (Preferred)

- Version specific upgrade notes - <https://github.com/munkireport/munkireport-php/wiki/How-to-Upgrade-Versions>
- General upgrade documentation - <https://github.com/munkireport/munkireport-php/wiki/General-Upgrade-Procedures>

If updating to the latest version is not possible:

- Update `munkireport-php/app/models/tablequery.php` to the version that ships with MR 5.3.0 - Replace that file with the one that you can download here: <https://github.com/munkireport/munkireport-php/blob/71d4de2898fde211e57d418a5b7750ed54aef6f3/app/models/tablequery.php> This should work for MunkiReport version 3.0.0 and up.

An Opensource project

► Pages 99

Introduction

- [Getting Started](#)
- [Demonstration Setup](#)
- [Demonstration Setup v6](#)

Setup

- Server Setup
 - Apache
 - NGINX
 - IIS
 - macOS Server
 - Docker
 - Reverse Proxies and Load Balancers
- .env Settings
- Client Setup
 - AutoPkg
- Database
 - SQLite
 - MySQL
- Jamf

Server Configuration

- Server Configuration
- Authentication
 - No Authentication
 - Local Authentication
 - LDAP-Authentication (AD, OpenLDAP, FreeIPA)
 - SAML Authentication
 - Shibboleth, CAS, ADFS Setup
 - Azure AD setup
 - Google Workspace setup
 - Okta setup
 - Network Authentication
- Authorization, Roles and Groups
- Business Units
- Machine Groups

Client Configuration

- [Client Configuration](#)
- [Client Runs](#)
- [Archiving Clients](#)

Upgrade

- [General Upgrade Procedures](#)
- [How to Upgrade Versions](#)

- [Troubleshooting Upgrades](#)
- [Migrating sqlite to MySQL](#)

Modules

- [Module Overview](#)
- [Module List](#)
 - [3rd Party/Beta Modules](#)
- [Module Marketplace](#)
- [Module Creation](#)
 - [Module Template](#)
- [Module YAML Conversion](#)

Securing MunkiReport

- [Client passphrase](#)
- [Secure the database](#)

Customization

- [Dashboards](#)
- [Client Summary Tab](#)
- [Themes](#)
- [Graphs](#)
- [Custom Widgets](#)
- [Customize the interface](#)
- [Hacking](#)

Misc

- [Common Issues](#)
- [Hotkeys](#)
- [Performance](#)
- [Troubleshooting](#)

Developers

- [Setting up a dev environment](#)
- [Localizing](#)
- [API](#)
- [Module listings](#)
- [Widget templates](#)
- [Caching data](#)
- [Python updates](#)

Clone this wiki locally

<https://github.com/munkireport/munkireport-php.wiki.git>

