20200309 Authenticated Comment XSS

Jump to bottom

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

Authenticated Comment XSS - CVE-2020-10191

Description

A logged in admin can craft a special request using his admin session credentials to inject javascript into a comment field. The javascript can be used to extract data from another admin that is logged in.

Vulnerability: Versions of MunkiReport from 2.5.3 to 5.2.x 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 in not possible:

- Update the `comment` module to v2.2 - only possible when running MunkiReport 4.3.0RC2 or higher.
- Or disable the `comment` module by removing it from the `MODULES=` setting in the server config.

- 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
```