

dev, Инвентаризация

Инвентаризация: DEV: Security

Сейчас большинство API запросов не требуют авторизации, надо сделать чтобы требовали (при включенном RBAC) С точки зрения безопасности у нас есть одна большая проблема: скрипт сбора информации с конечных ОС:

- он раскидан везде / доступен отовсюду
- работает от имени пользователя
- имеет права на запись в Инвентори

Если все остальные полномочия мы можем закрыть паролем, то в этом случае мы светим в скрипте пароль с правами чтения/записи в БД, что есть плохо Тогда:

1. Перестаем читать БД, просто бросаем сырые данные через API и возвращаем текст ошибки если таковая есть и ID ос
2. Создаем отдельную роль «comp-pusher», который может создавать/обновлять OS
3. Заводим служебного пользователя, с этой ролью
4. Хардкодим его в скрипт
5. Обновляем puppet-модуль puppet-inventory

Возможность/необходимость авторизации должна быть учтена в

- Скрипты инвентаризации ОС Windows - rest/domains, rest/comps
 - Библиотеки VBS для Inventory и HTTP
- Скрипты инвентаризации ОС Linux - rest/domains, rest/comps
- Скрипты инвентаризации ОС через PowerCLI - rest/techs,comps,domains
- Скрипты синхронизации пользователей с АД — ~~rest/users~~,partners,org-struct,phones
- Плагин интеграции DokuWiki с Inventory — ~~rest не используется, используются пользовательские маршруты~~
- Скрипт определителя номера для Asterisk — ~~rest/phones~~,**users**
- Скрипт определения дежурного техподдержки — ~~rest/schedules~~,**users**
- Скрипты генерации OpenVPN конфигов — ~~rest/users~~,net-ips
- Скрипты выдачи лицензий ПО (Офис, Siemens NX) - rest/lic-links

Оставшиеся контроллеры:

- comps
- contracts
- domains
- lic-keys
- lic-links
- login-journal
- ~~net-ips~~
- phones
- schedules
- services
- techs

From:
<http://wiki.reviakin.net/> - Wiki

Permanent link:
<http://wiki.reviakin.net/%D0%B8%D0%BD%D0%B2%D0%B5%D0%BD%D1%82%D0%B0%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F:dev:security?rev=1696841914>

Last update: 2023/10/09 08:58

