Аудит контракта MyERC20impliment

MyERC20impliment – контракт имплементация для реализации изменяемости логики контракта токена ERC20

1. Уязвимость функции инициализации

Описание: Функция initialize() может быть вызвана кем угодно, что позволяет злоумышленнику стать администратором.
Рекомендация: Ограничить вызов определенным адресом.

2. Вероятность коллизий при обращении в Storage

Описание: При использовании прокси контракта и имплементации могут возникать конфликты по слотам различных переменных, что может привести к потере данных.
Рекомендация: Наследование ERC20 имплементаций от contracts-/token/ERC20/ERC20Upgradeable.sol (отдельный пул контрактов для реализации имплементаций контрактов ERC20 от Openzeppelin), в которой уже заложен механизм создания отдельного пространства для данных контракта имплементации либо использовать свой механизм изоляции данных.

3. Проблемы управления ролями

Описание: В функции changeBurner() ошибочно отзывается MINTER_ROLE вместо BURNER_ROLE
Рекомендация: revokeRole(MINTER_ROLE, cb) изменить на revokeRole(BURNER_ROLE, cb) в строке 71

4. Отсутствие событий

Описание: Отсутствуют события для изменения минтера и бернера
Рекомендация: Добавить события при смене минтера и бернера.

Аудит контракта Proxy

Proxy – контракт реализующий прокси для контракта имплементации **MyERC20impliment**

1. Вероятность коллизий при обращении в Storage

Описание: Могут возникать конфликты с данными имплементации.
Рекомендация: Наследовать прокси контракт от contracts/proxy/ERC1967/ERC1967Proxy.sol (реализация прокси контрактов от Openzeppelin) либо использовать свой механизм изоляции данных.

2. Отсутствие проверок при обновлении

Описание: Не проверяется, что имплементация является контрактом.
Рекомендация: Проверка осуществляется при использовании contracts/proxy/ERC1967/ERC1967Proxy.sol (реализация прокси контрактов от Openzeppelin) либо необходимо реализовать свою проверку.

3. Невозможность смены админа

Описание: Контракт не предполагает сценария изменения администратора прокси контракта.
Рекомендация: Использовать реализацию contracts/proxy/ERC1967/ERC1967Proxy.sol (реализация прокси контрактов от Openzeppelin) либо сделать кастомную реализацию смены администратора.

4. Отсутствие событий

Описание: Нет события обновления имплементации.
Рекомендация: Добавить событие обновления имплементации.