[Audited]
https://etherscan.io/address/0x4aa42145Aa6Ebf72e164C9bBC74fbD3788045016#code
(EternalStorageProxy)
The above contract is a proxy for:
https://etherscan.io/address/0x166124b75c798Cedf1B43655E9B5284eBd5203DB#code
(XDaiForeignBridge)

Scope of Audit

The scope of this audit was to analyze and document the EternalStorageProxy & XDaiForeignBridge smart contracts for quality, security, correctness and any possible vulnerabilities.

Checked Vulnerabilities

- Access Management
- Arbitrary write to storage
- Centralization of control
- Ether theft
- Improper or missing events
- Logical issues and flaws
- Arithmetic Correctness
- Race conditions / front running
- SWC Registry
- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- Exception Disorder
- Gasless Send
- Use of tx.origin
- Malicious libraries
- Compiler version not fixed
- Address hardcoded
- Divide before multiply
- Integer overflow/underflow
- ERC's conformance
- Dangerous strict equalities
- Tautology or contradiction
- Return values of low-level calls
- Missing Zero Address Validation
- Private modifier
- Revert/require functions
- Multiple Sends
- Using suicide (As it is deprecated)
- Using delegatecall
- Upgradeable safety

- Using throw (As it is deprecated)
- Using inline assembly
- Style guide violation
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of the smart contracts, care was taken to ensure:

- The overall quality of the code in the contracts.
- Adherence to solidity’s best practices.
- Code documentation, comments, mathematical logic, expected behavior etc.
- Efficient usage of gas.
- Code safety from re-entrancy and other well known vulnerabilities.

The following techniques, methods, and tools were used to review all the smart contracts

Structural Analysis
In this stage, we meticulously analyzed the design patterns and structure of the smart contracts. Our objective was to ensure that the smart contract is meticulously structured to mitigate any potential issues that may arise in the future.

Static Analysis
A comprehensive static analysis of the smart contracts was conducted to identify potential vulnerabilities. This involved leveraging a range of automated tools to thoroughly assess the security posture of the smart contracts.

Code Review / Manual Analysis
Manual code analysis was conducted to uncover new vulnerabilities and validate those identified during static analysis. This involved a meticulous examination of the contracts, ensuring thorough coverage of potential risks. Additionally, the findings from automated analysis were manually verified to ensure accuracy and completeness.

Gas Consumption
We meticulously monitored gas consumption to identify areas for optimization and enhance efficiency. This involved analyzing code execution to pinpoint opportunities for reducing gas usage while maintaining optimal functionality.

Tools and Platforms used for Audit
Foundry, Solidity Visual Developer, Solhint, Slither, Static Analysis, Mythril
Issue Categories

Types of Severity

Each issue outlined in this report has been categorized according to its severity level, with four distinct classifications. Below, we have provided detailed explanations for each severity level to ensure clear understanding and appropriate action.

High Severity Issues

A high severity issue or vulnerability indicates a critical risk to your smart contract's security. These issues have the potential to be exploited, posing significant threats to the performance and functionality of the contract. It is strongly recommended to prioritize the resolution of these issues before deploying the contract in a live environment.

Medium Severity Issues

Medium severity issues typically stem from errors and deficiencies within the smart contract code. While they may not pose immediate critical risks, they have the potential to cause problems and should be addressed to ensure the contract's robustness and reliability.

Low Severity Issues

Low-level severity issues typically have minimal impact and serve as warnings rather than critical vulnerabilities. While they may not require immediate attention, it is advisable to address them at some point in the future to maintain the overall integrity and quality of the smart contract.

Informational

These levels indicate improvement requests, general questions, cosmetic or documentation errors, or requests for information. They have a low-to-no impact on the functionality or security of the smart contract.

Types of Issues

Open

Security vulnerabilities have been identified and must be resolved; however, they remain unresolved at present.

Resolved

These are the issues identified during the initial audit and have been successfully resolved.

Acknowledged

These are vulnerabilities that have been acknowledged but are pending resolution.

Partially Resolved

Significant efforts have been made to mitigate the risk/impact of the security issue, but it has not been fully resolved yet.

Introduction

XDaiForeignBridge inherits from ForeignBridgeErcToNative, SavingsDaiConnector, and GSNForeignERC20Bridge. The contract appears to be part of a bridge mechanism that allows for the transfer of ERC20 tokens (specifically DAI) between different blockchains or layers, with additional functionality for interacting with a savings mechanism (sDAI vault).

Issues Found

High Severity Issues

1. Unchecked transfer

The return value of transfer/transferFrom is not checked.

- [ ] ID-1 InterestConnector._transferInterest(address,uint256) ignores return value by ERC20(_token).transfer(receiver,_amount)

https://github.com/balajipachai/audit-challenge/blob/main/src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#L182-L193

```
function _transferInterest(address _token, uint256 _amount) internal {
        address receiver = interestReceiver(_token);
        require(receiver != address(0), "Receiver can't be Null");
        ERC20(_token).transfer(receiver, _amount);
        if (AddressUtils.isContract(receiver)) {
            IInterestReceiver(receiver).onInterestReceived(_token);
        }
       emit PaidInterest(_token, receiver, _amount);
    }
```

- [ ] ID-2 ForeignBridgeErcToNative.relayTokens(address,uint256) ignores return value by erc20token().transferFrom(msg.sender,address(this),_amount)

https://github.com/balajipachai/audit-challenge/blob/main/src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#L64-L75

```
function relayTokens(address _receiver, uint256 _amount) public {
        require(_receiver != bridgeContractOnOtherSide(), "Relayed to Bridge
address");
        require(_receiver != address(0), "Relayed to Null address");
        require(_receiver != address(this), "Relayed to this address");
        require(_amount > 0, "Relayed zero funds");
        require(withinLimit(_amount), "Exceeds bridge daily limit");
        addTotalSpentPerDay(getCurrentDay(), _amount);
        erc20token().transferFrom(msg.sender, address(this), _amount);
        emit UserRequestForAffirmation(_receiver, _amount);
    }
```

- [ ] ID-3 ERC20Bridge.relayTokens(address,uint256) ignores return value by erc20token().transferFrom(msg.sender,address(this),_amount)

https://github.com/balajipachai/audit-challenge/blob/main/src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.sol#L19-L28

```
function relayTokens(address _receiver, uint256 _amount) public {
        require(_receiver != address(0), "Receiver can't be Null");
        require(_receiver != address(this), "Receiver can't be the Bridge");
        require(_amount > 0, "Relayed zero tokens");
        require(withinLimit(_amount), "Relayed above limit");
        addTotalSpentPerDay(getCurrentDay(), _amount);
        erc20token().transferFrom(msg.sender, address(this), _amount);
        emit UserRequestForAffirmation(_receiver, _amount);
    }
```

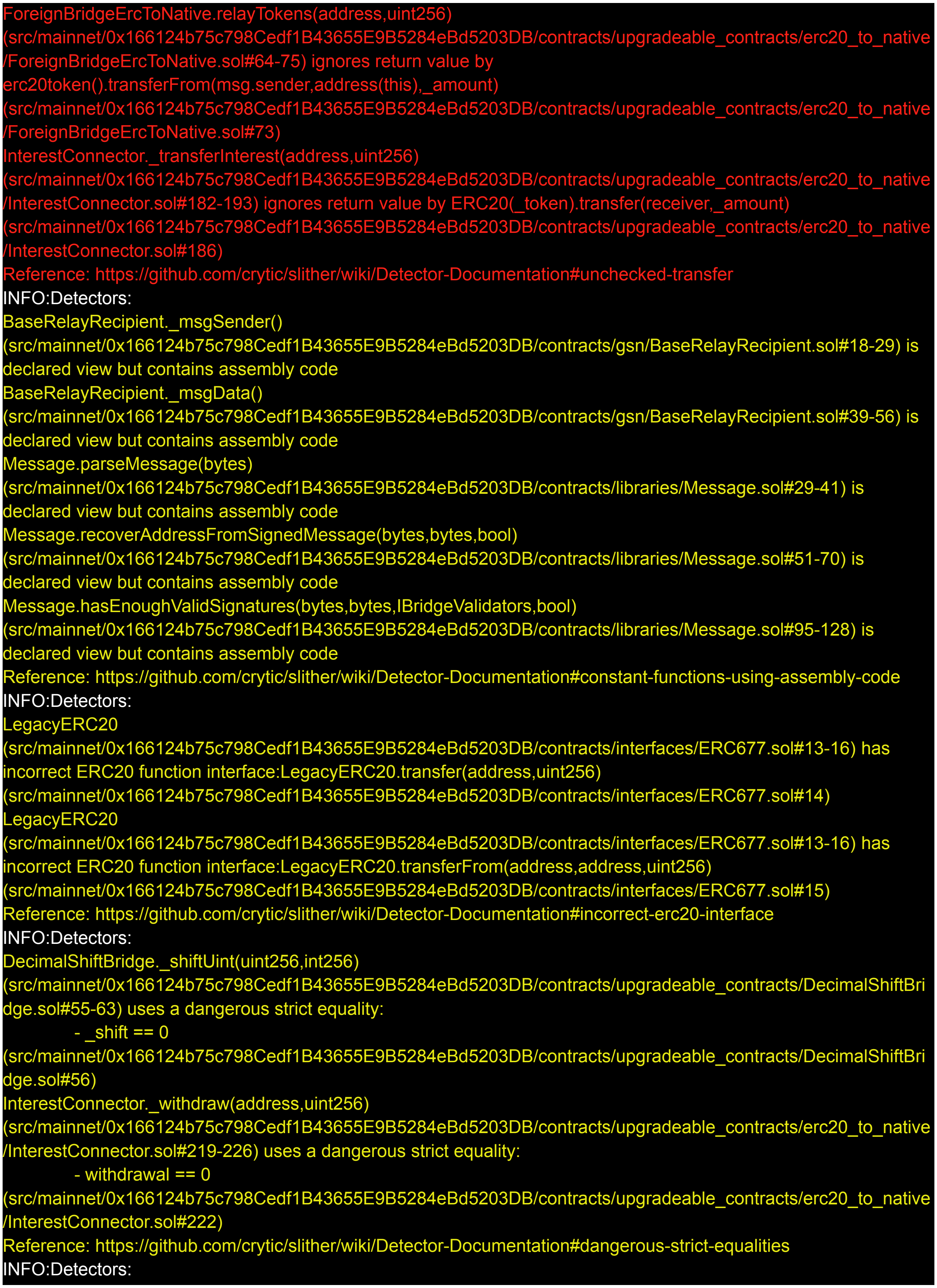
Several tokens do not revert in case of failure and return false.

Recommendation:

Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

Automated Tests Slither

```
INFO:Detectors:
SafeERC20.safeTransferFrom(address,address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#38-48) uses
arbitrary from in transferFrom: LegacyERC20(_token).transferFrom(_from,address(this),_value)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#39)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#arbitrary-from-in-transferfrom
INFO:Detectors:
ERC20Bridge.relayTokens(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#19-28) ignores return value by erc20token().transferFrom(msg.sender,address(this),_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#26)
```



```
ForeignBridgeErcToNative.relayTokens(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#64-75) ignores return value by
erc20token().transferFrom(msg.sender,address(this),_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#73)
InterestConnector._transferInterest(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#182-193) ignores return value by ERC20(_token).transfer(receiver,_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#186)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unchecked-transfer
INFO:Detectors:
BaseRelayRecipient._msgSender()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#18-29) is
declared view but contains assembly code
BaseRelayRecipient._msgData()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#39-56) is
declared view but contains assembly code
Message.parseMessage(bytes)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#29-41) is
declared view but contains assembly code
Message.recoverAddressFromSignedMessage(bytes,bytes,bool)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#51-70) is
declared view but contains assembly code
Message.hasEnoughValidSignatures(bytes,bytes,IBridgeValidators,bool)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#95-128) is
declared view but contains assembly code
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#constant-functions-using-assembly-code
INFO:Detectors:
LegacyERC20
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ERC677.sol#13-16) has
incorrect ERC20 function interface:LegacyERC20.transfer(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ERC677.sol#14)
LegacyERC20
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ERC677.sol#13-16) has
incorrect ERC20 function interface:LegacyERC20.transferFrom(address,address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ERC677.sol#15)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-erc20-interface
INFO:Detectors:
DecimalShiftBridge._shiftUint(uint256,int256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#55-63) uses a dangerous strict equality:
        - _shift == 0
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#56)
InterestConnector._withdraw(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#219-226) uses a dangerous strict equality:
        - withdrawal == 0
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#222)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dangerous-strict-equalities
INFO:Detectors:
```

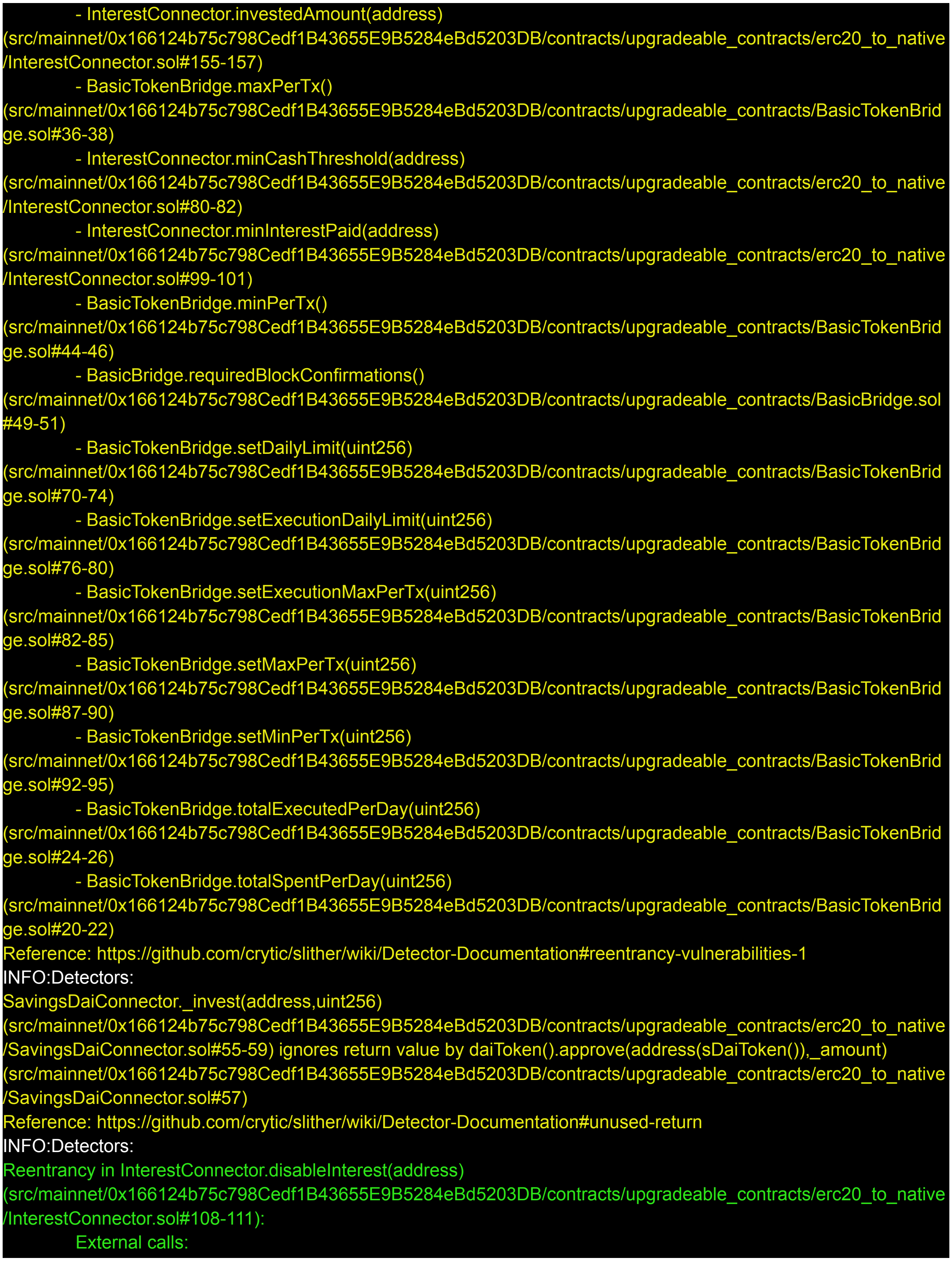
```
Reentrancy in InterestConnector._withdraw(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#219-226):
	External calls:
	- redeemed = _safeWithdrawTokens(_token,withdrawal)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#223)
		- ERC20(_token).balanceOf(address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#281)
	State variables written after the call(s):
	- _setInvestedAmount(_token,invested - redeemed)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#225)
		- uintStorage[keccak256()(abi.encodePacked(investedAmount,_token))] = _amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#210)
	EternalStorage.uintStorage
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeability/EternalStorage.sol#8)
can be used in cross function reentrancies:
	- BasicBridge._setGasPrice(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#57-60)
	- InterestConnector._setInvestedAmount(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#209-211)
	- InterestConnector._setMinCashThreshold(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#252-254)
	- InterestConnector._setMinInterestPaid(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#261-263)
	- BasicBridge._setRequiredBlockConfirmations(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#43-47)
	- BasicTokenBridge.addTotalSpentPerDay(uint256,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#62-64)
	- BasicTokenBridge.dailyLimit()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#28-30)
	- DecimalShiftBridge.decimalShift()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBridge.sol#27-29)
	- InitializableBridge.deployedAtBlock()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/InitializableBridge.sol#8-10)
	- BasicTokenBridge.executionDailyLimit()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#32-34)
	- BasicTokenBridge.executionMaxPerTx()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#40-42)
```

```
	- BasicBridge.gasPrice()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#35-37)
	- InterestConnector.investedAmount(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#155-157)
	- BasicTokenBridge.maxPerTx()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#36-38)
	- InterestConnector.minCashThreshold(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#80-82)
	- InterestConnector.minInterestPaid(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#99-101)
	- BasicTokenBridge.minPerTx()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#44-46)
	- BasicBridge.requiredBlockConfirmations()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#49-51)
	- BasicTokenBridge.setDailyLimit(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#70-74)
	- BasicTokenBridge.setExecutionDailyLimit(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#76-80)
	- BasicTokenBridge.setExecutionMaxPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#82-85)
	- BasicTokenBridge.setMaxPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#87-90)
	- BasicTokenBridge.setMinPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#92-95)
	- BasicTokenBridge.totalExecutedPerDay(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#24-26)
	- BasicTokenBridge.totalSpentPerDay(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#20-22)
	- _setInvestedAmount(_token,0)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#225)
		- uintStorage[keccak256()(abi.encodePacked(investedAmount,_token))] = _amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#210)
	EternalStorage.uintStorage
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeability/EternalStorage.sol#8)
can be used in cross function reentrancies:
	- BasicBridge._setGasPrice(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#57-60)
```

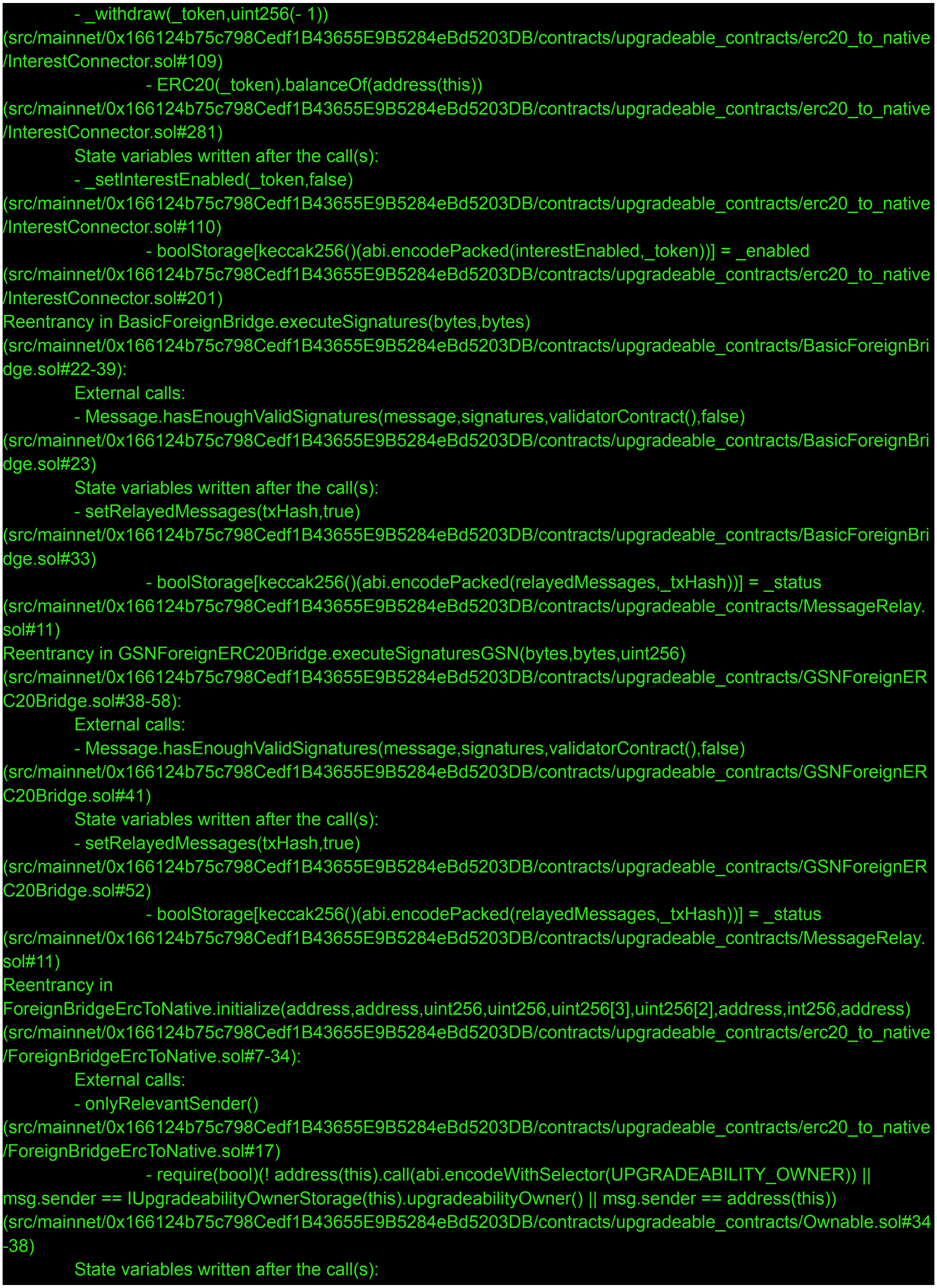
```
	- InterestConnector._setInvestedAmount(address,uint256) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#209-211)
	- InterestConnector._setMinCashThreshold(address,uint256) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#252-254)
	- InterestConnector._setMinInterestPaid(address,uint256) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#261-263)
	- BasicBridge._setRequiredBlockConfirmations(uint256) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#43-47)
	- BasicTokenBridge.addTotalSpentPerDay(uint256,uint256) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#62-64)
	- BasicTokenBridge.dailyLimit() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#28-30)
	- DecimalShiftBridge.decimalShift() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBridge.sol#27-29)
	- InitializableBridge.deployedAtBlock() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/InitializableBridge.sol#8-10)
	- BasicTokenBridge.executionDailyLimit() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#32-34)
	- BasicTokenBridge.executionMaxPerTx() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#40-42)
	- BasicBridge.gasPrice() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#35-37)
	- InterestConnector.investedAmount(address) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#155-157)
	- BasicTokenBridge.maxPerTx() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#36-38)
	- InterestConnector.minCashThreshold(address) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#80-82)
	- InterestConnector.minInterestPaid(address) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#99-101)
	- BasicTokenBridge.minPerTx() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#44-46)
	- BasicBridge.requiredBlockConfirmations() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#49-51)
	- BasicTokenBridge.setDailyLimit(uint256) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#70-74)
```

```
        - BasicTokenBridge.setExecutionDailyLimit(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#76-80)
        - BasicTokenBridge.setExecutionMaxPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#82-85)
        - BasicTokenBridge.setMaxPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#87-90)
        - BasicTokenBridge.setMinPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#92-95)
        - BasicTokenBridge.totalExecutedPerDay(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#24-26)
        - BasicTokenBridge.totalSpentPerDay(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#20-22)
Reentrancy in XDaiForeignBridge.onExecuteMessageGSN(address,uint256,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#85-89):
        External calls:
        - ensureEnoughTokens(daiToken(),amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#86)
                - currentBalance = token.balanceOf(address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#92)
                - ERC20(_token).balanceOf(address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#281)
                - require(bool,string)(sDaiToken().withdraw(_amount,address(this),address(this)) > 0,Failed to
withdraw)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/SavingsDaiConnector.sol#69)
        - super.onExecuteMessageGSN(recipient,amount,fee)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#88)
                - first = token.transfer(addressStorage[PAYMASTER],fee)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#64)
                - second = token.transfer(recipient,amount - fee)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#65)
        State variables written after the call(s):
        - super.onExecuteMessageGSN(recipient,amount,fee)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#88)
                - uintStorage[keccak256()(abi.encodePacked(totalExecutedPerDay,_day))] =
totalExecutedPerDay(_day).add(_value)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#67)
```

```
	EternalStorage.uintStorage
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeability/EternalStorage.sol#8)
can be used in cross function reentrancies:
	- BasicTokenBridge._setExecutionLimits(uint256[2])
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#123-130)
	- BasicBridge._setGasPrice(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#57-60)
	- InterestConnector._setInvestedAmount(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#209-211)
	- BasicTokenBridge._setLimits(uint256[3])
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#109-121)
	- InterestConnector._setMinCashThreshold(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#252-254)
	- InterestConnector._setMinInterestPaid(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#261-263)
	- BasicBridge._setRequiredBlockConfirmations(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#43-47)
	- BasicTokenBridge.addTotalExecutedPerDay(uint256,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#66-68)
	- BasicTokenBridge.addTotalSpentPerDay(uint256,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#62-64)
	- BasicTokenBridge.dailyLimit()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#28-30)
	- DecimalShiftBridge.decimalShift()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#27-29)
	- InitializableBridge.deployedAtBlock()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/InitializableBridg
e.sol#8-10)
	- BasicTokenBridge.executionDailyLimit()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#32-34)
	- BasicTokenBridge.executionMaxPerTx()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#40-42)
	- BasicBridge.gasPrice()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#35-37)
	-
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#8-35)
```



```
	- InterestConnector.investedAmount(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#155-157)
	- BasicTokenBridge.maxPerTx()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#36-38)
	- InterestConnector.minCashThreshold(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#80-82)
	- InterestConnector.minInterestPaid(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#99-101)
	- BasicTokenBridge.minPerTx()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#44-46)
	- BasicBridge.requiredBlockConfirmations()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#49-51)
	- BasicTokenBridge.setDailyLimit(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#70-74)
	- BasicTokenBridge.setExecutionDailyLimit(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#76-80)
	- BasicTokenBridge.setExecutionMaxPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#82-85)
	- BasicTokenBridge.setMaxPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#87-90)
	- BasicTokenBridge.setMinPerTx(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#92-95)
	- BasicTokenBridge.totalExecutedPerDay(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#24-26)
	- BasicTokenBridge.totalSpentPerDay(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#20-22)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-1
INFO:Detectors:
SavingsDaiConnector._invest(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/SavingsDaiConnector.sol#55-59) ignores return value by daiToken().approve(address(sDaiToken()),_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/SavingsDaiConnector.sol#57)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
INFO:Detectors:
Reentrancy in InterestConnector.disableInterest(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#108-111):
	External calls:
```



```
        - _withdraw(_token,uint256(- 1))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#109)
                - ERC20(_token).balanceOf(address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#281)
        State variables written after the call(s):
        - _setInterestEnabled(_token,false)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#110)
                - boolStorage[keccak256()(abi.encodePacked(interestEnabled,_token))] = _enabled
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#201)
Reentrancy in BasicForeignBridge.executeSignatures(bytes,bytes)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicForeignBri
dge.sol#22-39):
        External calls:
        - Message.hasEnoughValidSignatures(message,signatures,validatorContract(),false)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicForeignBri
dge.sol#23)
        State variables written after the call(s):
        - setRelayedMessages(txHash,true)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicForeignBri
dge.sol#33)
                - boolStorage[keccak256()(abi.encodePacked(relayedMessages,_txHash))] = _status
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/MessageRelay.
sol#11)
Reentrancy in GSNForeignERC20Bridge.executeSignaturesGSN(bytes,bytes,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#38-58):
        External calls:
        - Message.hasEnoughValidSignatures(message,signatures,validatorContract(),false)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#41)
        State variables written after the call(s):
        - setRelayedMessages(txHash,true)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#52)
                - boolStorage[keccak256()(abi.encodePacked(relayedMessages,_txHash))] = _status
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/MessageRelay.
sol#11)
Reentrancy in
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#7-34):
        External calls:
        - onlyRelevantSender()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#17)
                - require(bool)(! address(this).call(abi.encodeWithSelector(UPGRADEABILITY_OWNER)) ||
msg.sender == IUpgradeabilityOwnerStorage(this).upgradeabilityOwner() || msg.sender == address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#34
-38)
        State variables written after the call(s):
```

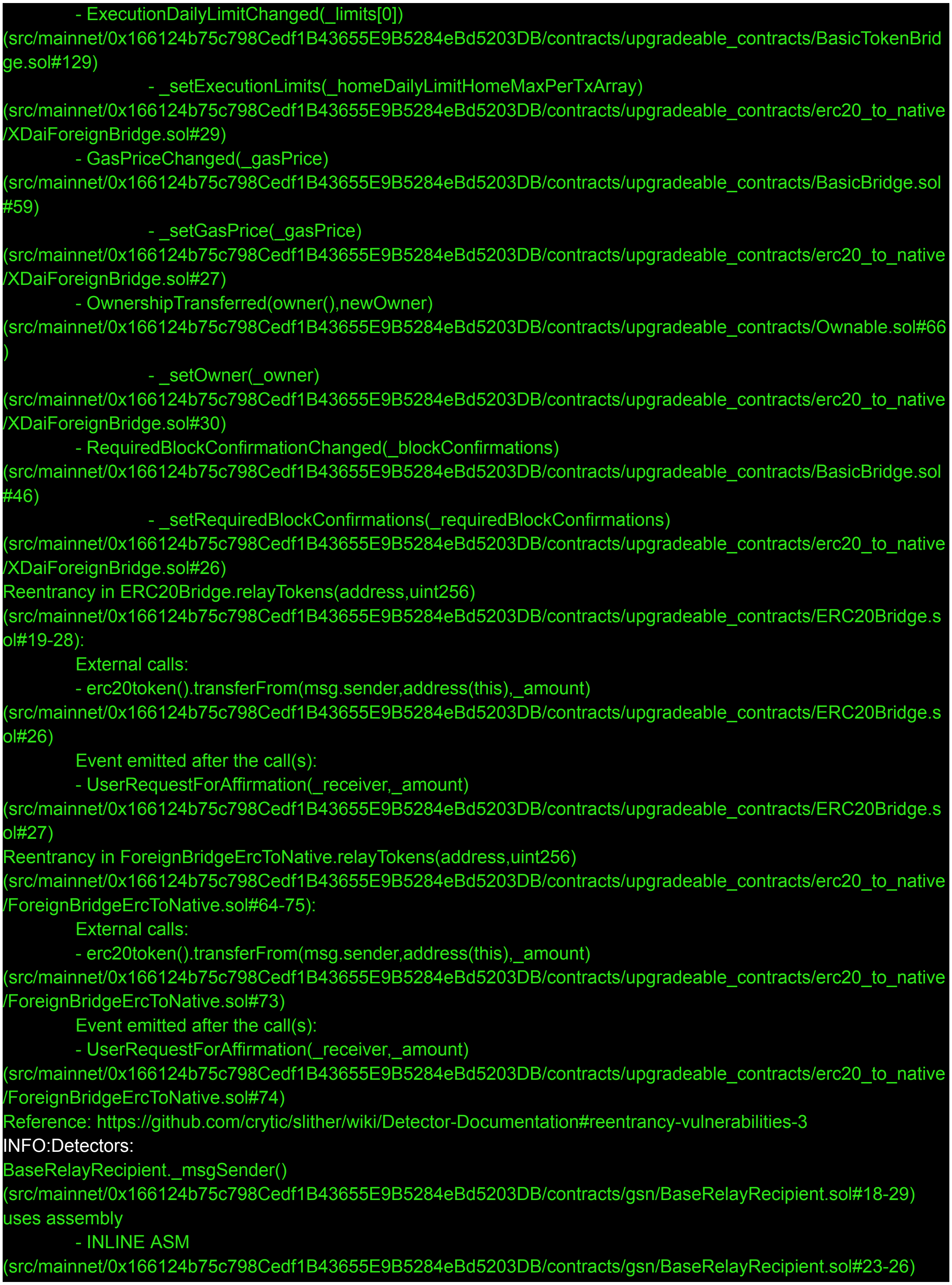
```
		- addressStorage[VALIDATOR_CONTRACT] = _validatorContract (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#21)
	- setErc20token(_erc20token) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#22)
		- addressStorage[ERC20_TOKEN] = _token (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.sol#16)
	- _setOwner(_owner) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#29)
		- addressStorage[OWNER] = newOwner (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#67)
	- _setBridgeContractOnOtherSide(_bridgeOnOtherSide) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#30)
		- addressStorage[BRIDGE_CONTRACT] = _bridgeContract (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/OtherSideBridgeStorage.sol#10)
	- setInitialize() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#31)
		- boolStorage[INITIALIZED] = true (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Initializable.sol#9)
	- uintStorage[DEPLOYED_AT_BLOCK] = block.number (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#23)
	- _setRequiredBlockConfirmations(_requiredBlockConfirmations) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#24)
		- uintStorage[REQUIRED_BLOCK_CONFIRMATIONS] = _blockConfirmations (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#45)
	- _setGasPrice(_gasPrice) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#25)
		- uintStorage[GAS_PRICE] = _gasPrice (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#58)
	- _setLimits(_dailyLimitMaxPerTxMinPerTxArray) (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#26)
		- uintStorage[DAILY_LIMIT] = _limits[0] (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#116)
		- uintStorage[MAX_PER_TX] = _limits[1] (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#117)
		- uintStorage[MIN_PER_TX] = _limits[2] (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#118)
```

```
        - _setExecutionLimits(_homeDailyLimitHomeMaxPerTxArray)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#27)
                - uintStorage[EXECUTION_DAILY_LIMIT] = _limits[0]
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#126)
                - uintStorage[EXECUTION_MAX_PER_TX] = _limits[1]
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#127)
        - _setDecimalShift(_decimalShift)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#28)
                - uintStorage[DECIMAL_SHIFT] = uint256(_shift)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBridge.sol#20)
Reentrancy in
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#8-35):
        External calls:
        - onlyRelevantSender()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#18)
                - require(bool)(! address(this).call(abi.encodeWithSelector(UPGRADEABILITY_OWNER)) ||
msg.sender == IUpgradeabilityOwnerStorage(this).upgradeabilityOwner() || msg.sender == address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#34-38)
        State variables written after the call(s):
        - addressStorage[VALIDATOR_CONTRACT] = _validatorContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#24)
        - _setOwner(_owner)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#30)
                - addressStorage[OWNER] = newOwner
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#67)
        - _setBridgeContractOnOtherSide(_bridgeOnOtherSide)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#31)
                - addressStorage[BRIDGE_CONTRACT] = _bridgeContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/OtherSideBridgeStorage.sol#10)
        - setInitialize()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#32)
                - boolStorage[INITIALIZED] = true
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Initializable.sol#9)
        - uintStorage[DEPLOYED_AT_BLOCK] = block.number
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#25)
```

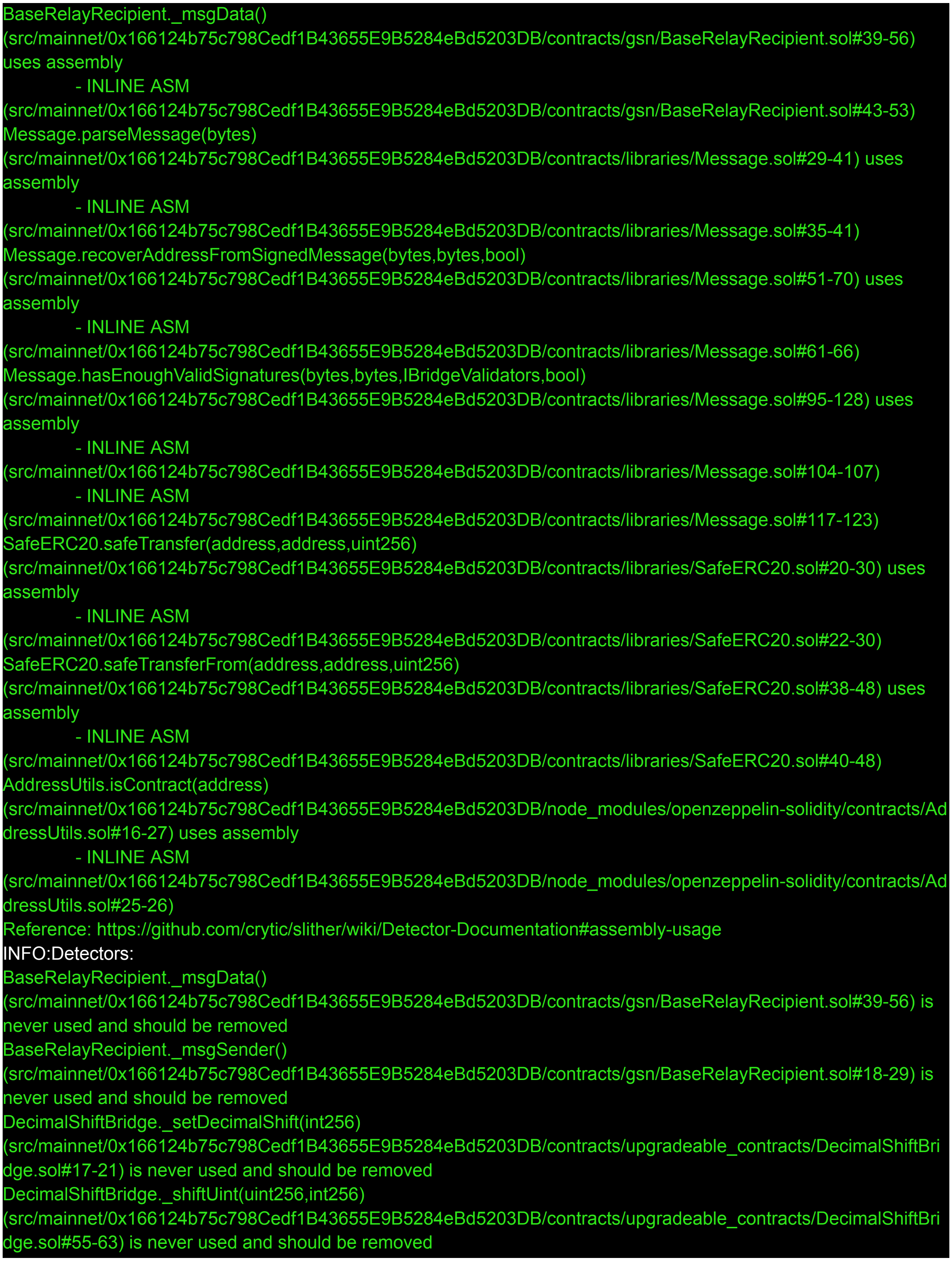
```
        - _setRequiredBlockConfirmations(_requiredBlockConfirmations)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#26)
                - uintStorage[REQUIRED_BLOCK_CONFIRMATIONS] = _blockConfirmations
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#45)
        - _setGasPrice(_gasPrice)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#27)
                - uintStorage[GAS_PRICE] = _gasPrice
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#58)
        - _setLimits(_dailyLimitMaxPerTxMinPerTxArray)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#28)
                - uintStorage[DAILY_LIMIT] = _limits[0]
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#116)
                - uintStorage[MAX_PER_TX] = _limits[1]
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#117)
                - uintStorage[MIN_PER_TX] = _limits[2]
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#118)
        - _setExecutionLimits(_homeDailyLimitHomeMaxPerTxArray)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#29)
                - uintStorage[EXECUTION_DAILY_LIMIT] = _limits[0]
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#126)
                - uintStorage[EXECUTION_MAX_PER_TX] = _limits[1]
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#127)
Reentrancy in InterestConnector.invest(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#164-174):
        External calls:
        - balance = _selfBalance(_token)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#165)
                - ERC20(_token).balanceOf(address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#281)
        State variables written after the call(s):
        - _setInvestedAmount(_token,investedAmount(_token).add(amount))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#171)
                - uintStorage[keccak256()(abi.encodePacked(investedAmount,_token))] = _amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#210)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
INFO:Detectors:
```

```
Reentrancy in InterestConnector._transferInterest(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#182-193):
        External calls:
        - ERC20(_token).transfer(receiver,_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#186)
        - IInterestReceiver(receiver).onInterestReceived(_token)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#189)
        Event emitted after the call(s):
        - PaidInterest(_token,receiver,_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#192)
Reentrancy in BasicForeignBridge.executeSignatures(bytes,bytes)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicForeignBri
dge.sol#22-39):
        External calls:
        - Message.hasEnoughValidSignatures(message,signatures,validatorContract(),false)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicForeignBri
dge.sol#23)
        Event emitted after the call(s):
        - RelayedMessage(recipient,amount,txHash)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicForeignBri
dge.sol#35)
Reentrancy in GSNForeignERC20Bridge.executeSignaturesGSN(bytes,bytes,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#38-58):
        External calls:
        - Message.hasEnoughValidSignatures(message,signatures,validatorContract(),false)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#41)
        - require(bool)(onExecuteMessageGSN(recipient,amount,maxTokensFee))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#53)
                - first = token.transfer(addressStorage[PAYMASTER],fee)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#64)
                - second = token.transfer(recipient,amount - fee)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#65)
        Event emitted after the call(s):
        - RelayedMessage(recipient,amount,txHash)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#54)
Reentrancy in
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#7-34):
        External calls:
        - onlyRelevantSender()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#17)
```

```
                - require(bool)(! address(this).call(abi.encodeWithSelector(UPGRADEABILITY_OWNER)) ||
msg.sender == IUpgradeabilityOwnerStorage(this).upgradeabilityOwner() || msg.sender == address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#34
-38)
        Event emitted after the call(s):
        - DailyLimitChanged(_limits[0])
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#120)
                - _setLimits(_dailyLimitMaxPerTxMinPerTxArray)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#26)
        - ExecutionDailyLimitChanged(_limits[0])
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#129)
                - _setExecutionLimits(_homeDailyLimitHomeMaxPerTxArray)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#27)
        - GasPriceChanged(_gasPrice)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#59)
                - _setGasPrice(_gasPrice)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#25)
        - OwnershipTransferred(owner(),newOwner)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#66
)
                - _setOwner(_owner)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#29)
        - RequiredBlockConfirmationChanged(_blockConfirmations)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#46)
                - _setRequiredBlockConfirmations(_requiredBlockConfirmations)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#24)
Reentrancy in
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#8-35):
        External calls:
        - onlyRelevantSender()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#18)
                - require(bool)(! address(this).call(abi.encodeWithSelector(UPGRADEABILITY_OWNER)) ||
msg.sender == IUpgradeabilityOwnerStorage(this).upgradeabilityOwner() || msg.sender == address(this))
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#34
-38)
        Event emitted after the call(s):
        - DailyLimitChanged(_limits[0])
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#120)
                - _setLimits(_dailyLimitMaxPerTxMinPerTxArray)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#28)
```



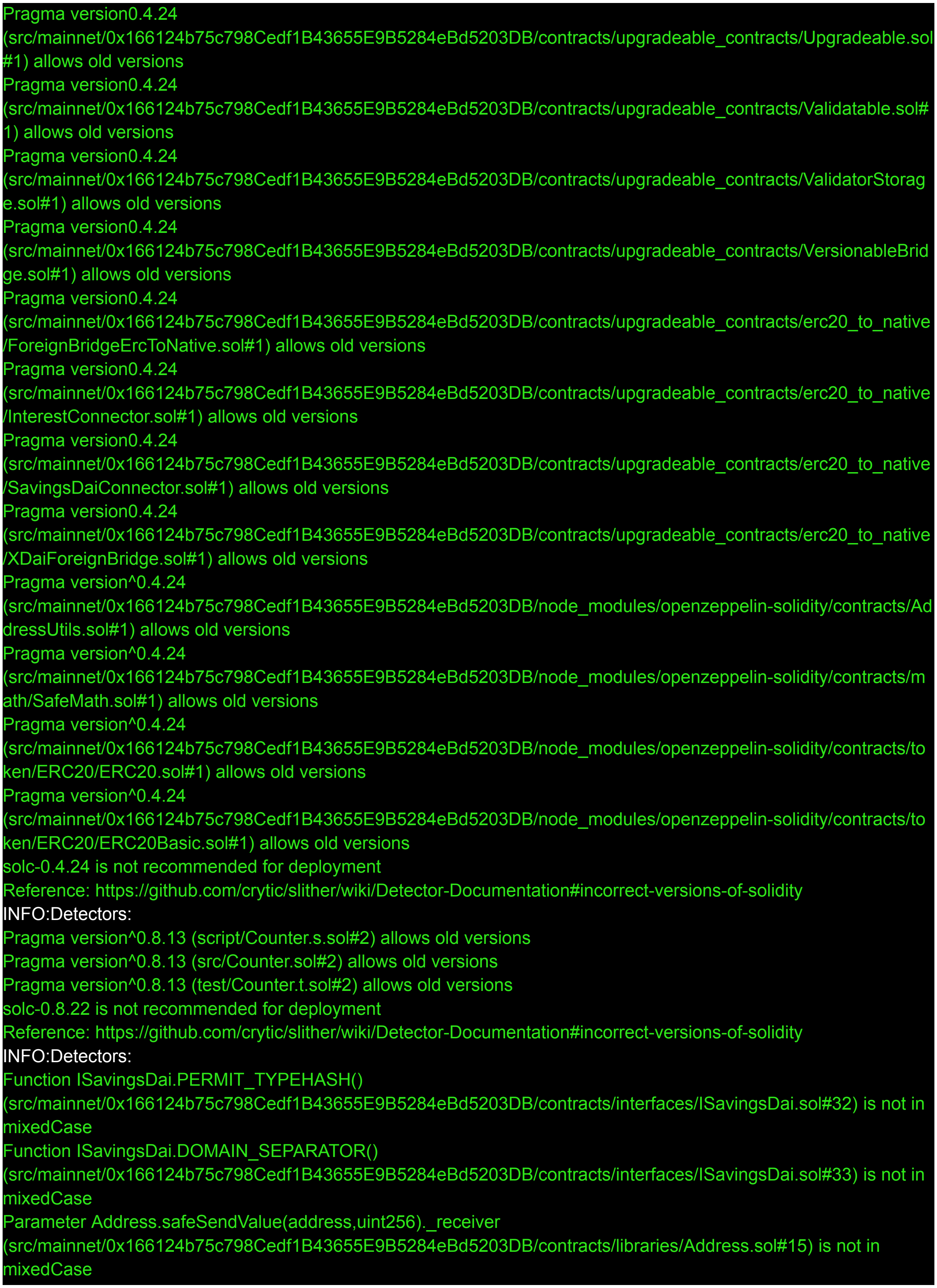
```
	- ExecutionDailyLimitChanged(_limits[0])
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBridge.sol#129)
		- _setExecutionLimits(_homeDailyLimitHomeMaxPerTxArray)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#29)
	- GasPriceChanged(_gasPrice)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#59)
		- _setGasPrice(_gasPrice)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#27)
	- OwnershipTransferred(owner(),newOwner)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#66)
		- _setOwner(_owner)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#30)
	- RequiredBlockConfirmationChanged(_blockConfirmations)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol#46)
		- _setRequiredBlockConfirmations(_requiredBlockConfirmations)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#26)
Reentrancy in ERC20Bridge.relayTokens(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.sol#19-28):
	External calls:
	- erc20token().transferFrom(msg.sender,address(this),_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.sol#26)
	Event emitted after the call(s):
	- UserRequestForAffirmation(_receiver,_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.sol#27)
Reentrancy in ForeignBridgeErcToNative.relayTokens(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#64-75):
	External calls:
	- erc20token().transferFrom(msg.sender,address(this),_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#73)
	Event emitted after the call(s):
	- UserRequestForAffirmation(_receiver,_amount)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#74)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
BaseRelayRecipient._msgSender()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#18-29)
uses assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#23-26)
```



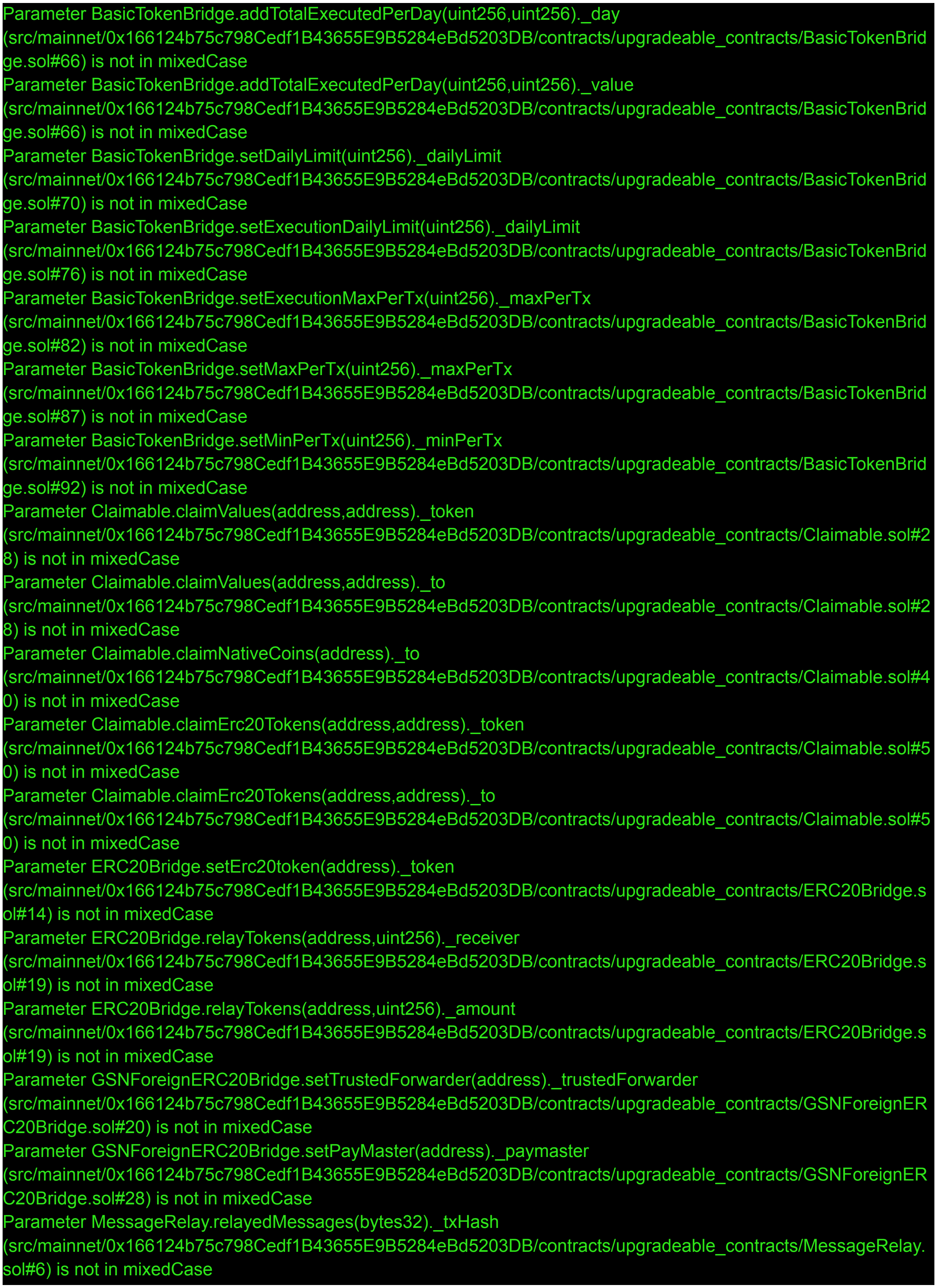
```
BaseRelayRecipient._msgData()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#39-56)
uses assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#43-53)
Message.parseMessage(bytes)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#29-41) uses
assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#35-41)
Message.recoverAddressFromSignedMessage(bytes,bytes,bool)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#51-70) uses
assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#61-66)
Message.hasEnoughValidSignatures(bytes,bytes,IBridgeValidators,bool)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#95-128) uses
assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#104-107)
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#117-123)
SafeERC20.safeTransfer(address,address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#20-30) uses
assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#22-30)
SafeERC20.safeTransferFrom(address,address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#38-48) uses
assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#40-48)
AddressUtils.isContract(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/Ad
dressUtils.sol#16-27) uses assembly
	- INLINE ASM
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/Ad
dressUtils.sol#25-26)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
BaseRelayRecipient._msgData()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#39-56) is
never used and should be removed
BaseRelayRecipient._msgSender()
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#18-29) is
never used and should be removed
DecimalShiftBridge._setDecimalShift(int256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#17-21) is never used and should be removed
DecimalShiftBridge._shiftUint(uint256,int256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#55-63) is never used and should be removed
```

```
DecimalShiftBridge._shiftValue(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#45-47) is never used and should be removed
DecimalShiftBridge._unshiftValue(uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#36-38) is never used and should be removed
ERC20Bridge.setErc20token(address)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#14-17) is never used and should be removed
ForeignBridgeErcToNative.onExecuteMessage(address,uint256,bytes32)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#51-58) is never used and should be removed
InterestConnector._transferInterest(address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#182-193) is never used and should be removed
Message.recoverAddressFromSignedMessage(bytes,bytes,bool)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#51-70) is never
used and should be removed
SafeERC20.safeTransferFrom(address,address,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#38-48) is
never used and should be removed
SafeMath.div(uint256,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#29-34) is never used and should be removed
SafeMath.mul(uint256,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#13-24) is never used and should be removed
SafeMath.sub(uint256,uint256)
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#39-42) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/BaseRelayRecipient.sol#3) allows
old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/interfaces/IKnowForwarderAddress
.sol#2) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/gsn/interfaces/IRelayRecipient.sol#2)
allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ERC677.sol#1) allows old
versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/IBridgeValidators.sol#1)
allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/IInterestReceiver.sol#1)
allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ISavingsDai.sol#18) allows
old versions
```

```
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/IUpgradeabilityOwnerStorage
.sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Address.sol#1) allows old
versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#1) allows old
versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#1) allows old
versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeability/EternalStorage.sol#1)
allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicForeignBri
dge.sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Claimable.sol#1
) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Initializable.sol#
1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/InitializableBridg
e.sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/MessageRelay.
sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/OtherSideBridg
eStorage.sol#1) allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Ownable.sol#1)
allows old versions
Pragma version0.4.24
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Sacrifice.sol#1)
allows old versions
```

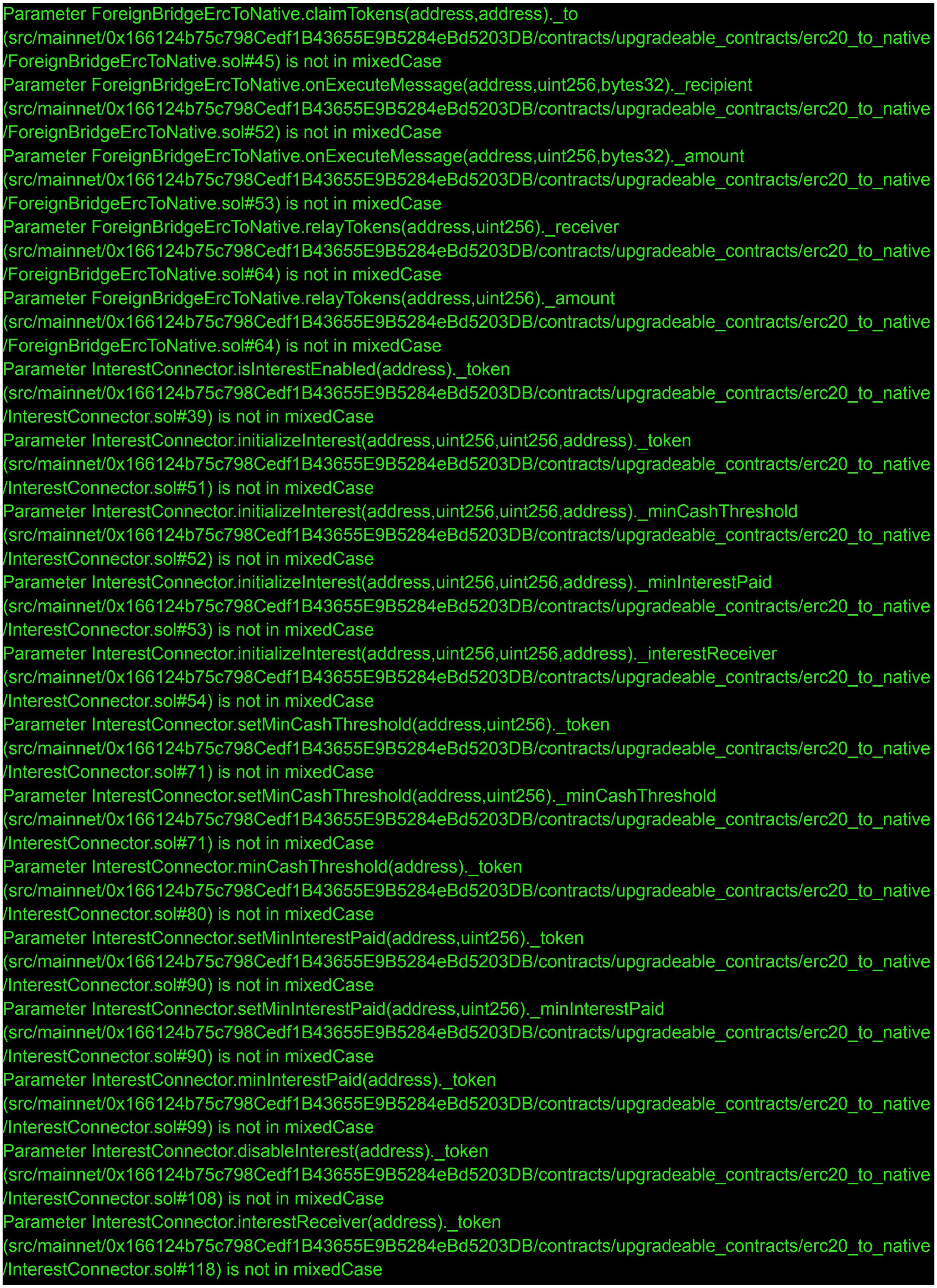


```
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Upgradeable.sol#1) allows old versions
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Validatable.sol#1) allows old versions
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ValidatorStorage.sol#1) allows old versions
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/VersionableBridge.sol#1) allows old versions
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/ForeignBridgeErcToNative.sol#1) allows old versions
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/InterestConnector.sol#1) allows old versions
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/SavingsDaiConnector.sol#1) allows old versions
Pragma version0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native/XDaiForeignBridge.sol#1) allows old versions
Pragma version^0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/AddressUtils.sol#1) allows old versions
Pragma version^0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/math/SafeMath.sol#1) allows old versions
Pragma version^0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/token/ERC20/ERC20.sol#1) allows old versions
Pragma version^0.4.24 (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/token/ERC20/ERC20Basic.sol#1) allows old versions
solc-0.4.24 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Pragma version^0.8.13 (script/Counter.s.sol#2) allows old versions
Pragma version^0.8.13 (src/Counter.sol#2) allows old versions
Pragma version^0.8.13 (test/Counter.t.sol#2) allows old versions
solc-0.8.22 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Function ISavingsDai.PERMIT_TYPEHASH() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ISavingsDai.sol#32) is not in mixedCase
Function ISavingsDai.DOMAIN_SEPARATOR() (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/interfaces/ISavingsDai.sol#33) is not in mixedCase
Parameter Address.safeSendValue(address,uint256)._receiver (src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Address.sol#15) is not in mixedCase
Parameter Address.safeSendValue(address,uint256)._value
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Address.sol#15) is not in
mixedCase
Parameter Message.isMessageValid(bytes)._msg
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#43) is not in
mixedCase
Parameter Message.hasEnoughValidSignatures(bytes,bytes,IBridgeValidators,bool)._message
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#96) is not in
mixedCase
Parameter Message.hasEnoughValidSignatures(bytes,bytes,IBridgeValidators,bool)._validatorContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/Message.sol#98) is not in
mixedCase
Parameter SafeERC20.safeTransfer(address,address,uint256)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#20) is not in
mixedCase
Parameter SafeERC20.safeTransfer(address,address,uint256)._to
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#20) is not in
mixedCase
Parameter SafeERC20.safeTransfer(address,address,uint256)._value
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#20) is not in
mixedCase
Parameter SafeERC20.safeTransferFrom(address,address,uint256)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#38) is not in
mixedCase
Parameter SafeERC20.safeTransferFrom(address,address,uint256)._from
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#38) is not in
mixedCase
Parameter SafeERC20.safeTransferFrom(address,address,uint256)._value
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/libraries/SafeERC20.sol#38) is not in
mixedCase
Parameter BasicBridge.setGasPrice(uint256)._gasPrice
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#31) is not in mixedCase
Parameter BasicBridge.setRequiredBlockConfirmations(uint256)._blockConfirmations
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicBridge.sol
#39) is not in mixedCase
Parameter BasicTokenBridge.totalSpentPerDay(uint256)._day
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#20) is not in mixedCase
Parameter BasicTokenBridge.totalExecutedPerDay(uint256)._day
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#24) is not in mixedCase
Parameter BasicTokenBridge.withinLimit(uint256)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#48) is not in mixedCase
Parameter BasicTokenBridge.withinExecutionLimit(uint256)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#53) is not in mixedCase
Parameter BasicTokenBridge.addTotalSpentPerDay(uint256,uint256)._day
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#62) is not in mixedCase
Parameter BasicTokenBridge.addTotalSpentPerDay(uint256,uint256)._value
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#62) is not in mixedCase
```

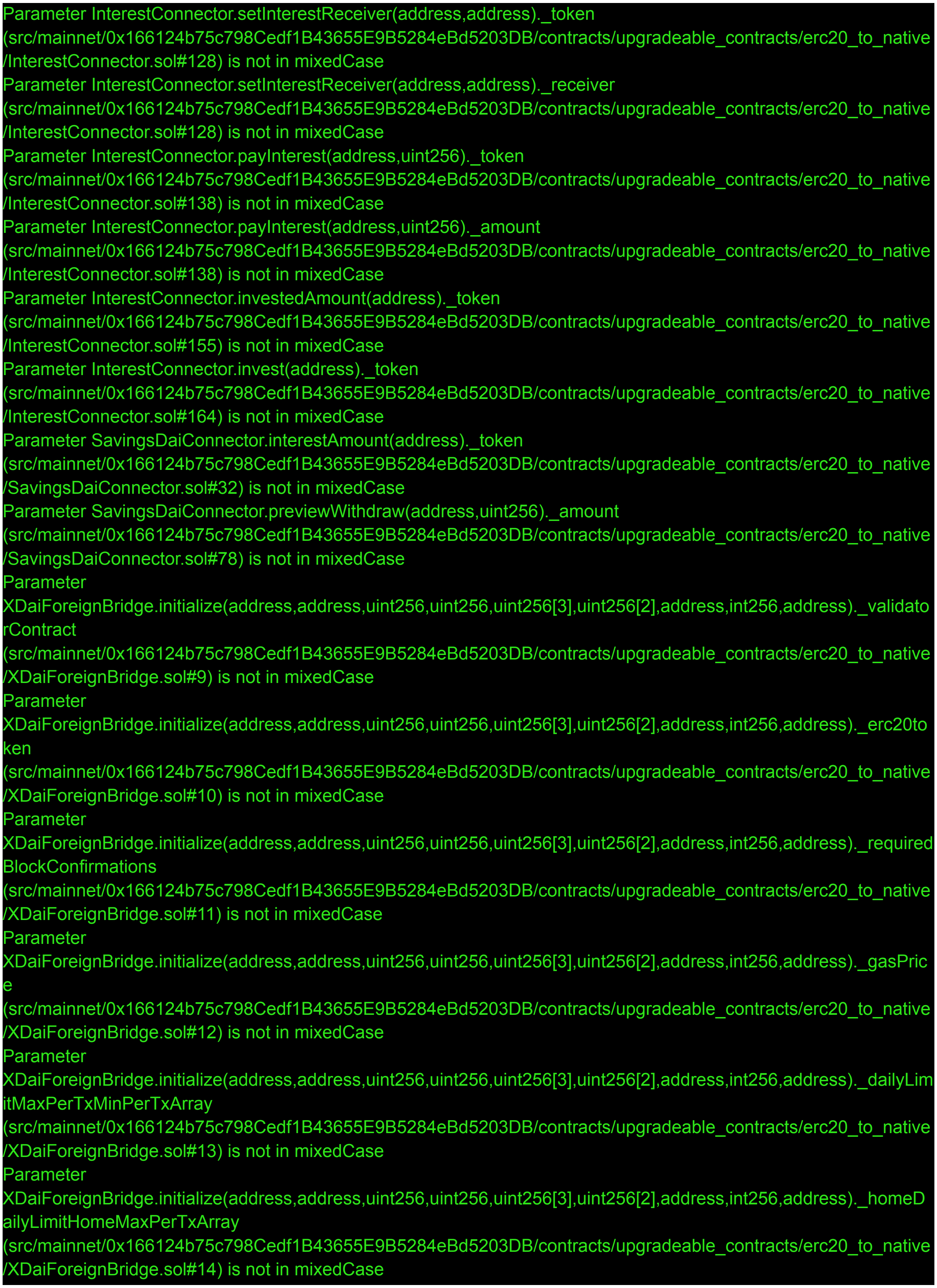


```
Parameter BasicTokenBridge.addTotalExecutedPerDay(uint256,uint256)._day
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#66) is not in mixedCase
Parameter BasicTokenBridge.addTotalExecutedPerDay(uint256,uint256)._value
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#66) is not in mixedCase
Parameter BasicTokenBridge.setDailyLimit(uint256)._dailyLimit
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#70) is not in mixedCase
Parameter BasicTokenBridge.setExecutionDailyLimit(uint256)._dailyLimit
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#76) is not in mixedCase
Parameter BasicTokenBridge.setExecutionMaxPerTx(uint256)._maxPerTx
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#82) is not in mixedCase
Parameter BasicTokenBridge.setMaxPerTx(uint256)._maxPerTx
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#87) is not in mixedCase
Parameter BasicTokenBridge.setMinPerTx(uint256)._minPerTx
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#92) is not in mixedCase
Parameter Claimable.claimValues(address,address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Claimable.sol#2
8) is not in mixedCase
Parameter Claimable.claimValues(address,address)._to
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Claimable.sol#2
8) is not in mixedCase
Parameter Claimable.claimNativeCoins(address)._to
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Claimable.sol#4
0) is not in mixedCase
Parameter Claimable.claimErc20Tokens(address,address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Claimable.sol#5
0) is not in mixedCase
Parameter Claimable.claimErc20Tokens(address,address)._to
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/Claimable.sol#5
0) is not in mixedCase
Parameter ERC20Bridge.setErc20token(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#14) is not in mixedCase
Parameter ERC20Bridge.relayTokens(address,uint256)._receiver
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#19) is not in mixedCase
Parameter ERC20Bridge.relayTokens(address,uint256)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#19) is not in mixedCase
Parameter GSNForeignERC20Bridge.setTrustedForwarder(address)._trustedForwarder
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#20) is not in mixedCase
Parameter GSNForeignERC20Bridge.setPayMaster(address)._paymaster
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#28) is not in mixedCase
Parameter MessageRelay.relayedMessages(bytes32)._txHash
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/MessageRelay.
sol#6) is not in mixedCase
```

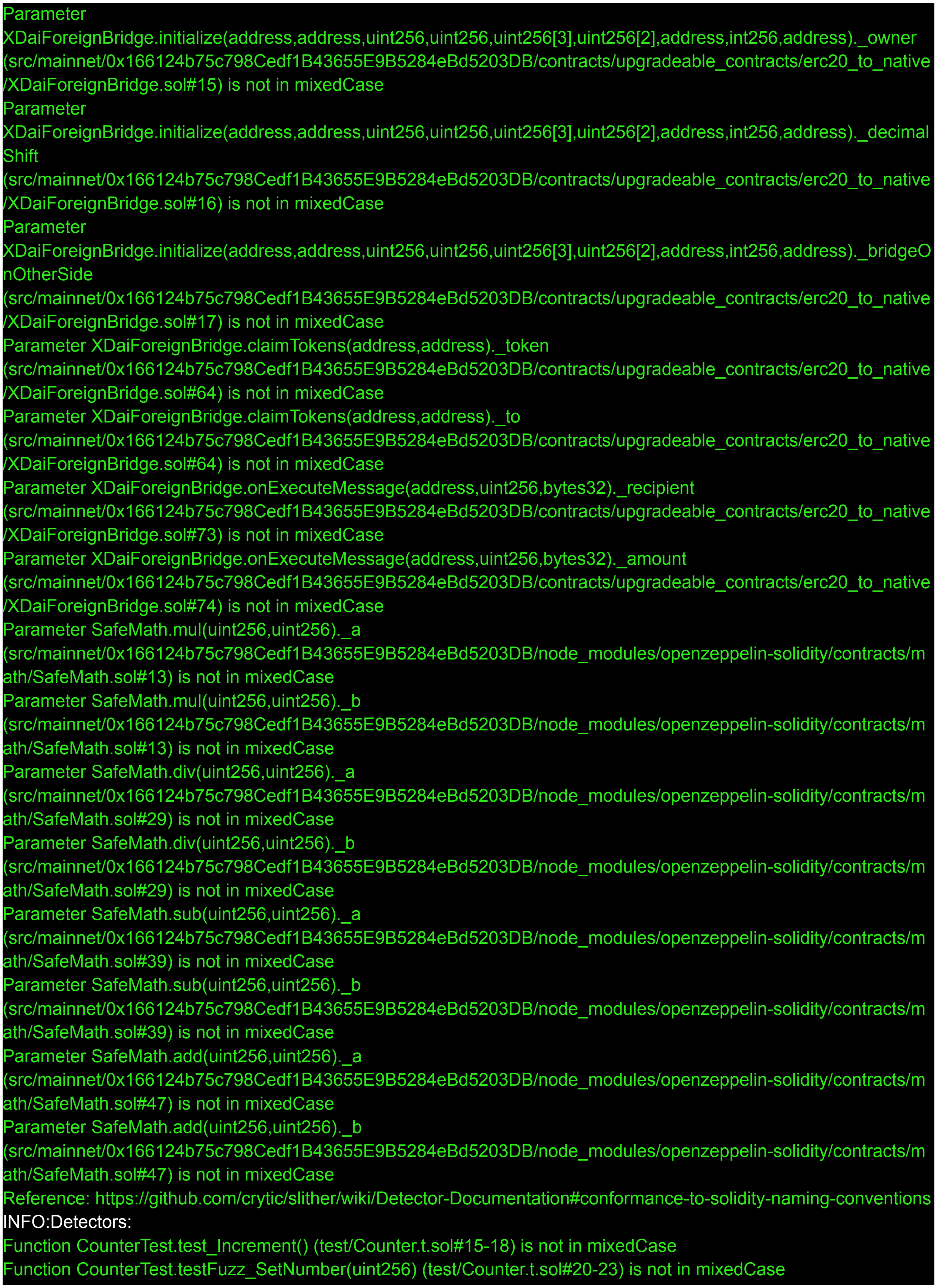
```
Parameter MessageRelay.setRelayedMessages(bytes32,bool)._txHash
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/MessageRelay.
sol#10) is not in mixedCase
Parameter MessageRelay.setRelayedMessages(bytes32,bool)._status
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/MessageRelay.
sol#10) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
validatorContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#8) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
erc20token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#9) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._r
equiredBlockConfirmations
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#10) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
gasPrice
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#11) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
dailyLimitMaxPerTxMinPerTxArray
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#12) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
homeDailyLimitHomeMaxPerTxArray
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#13) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
owner
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#14) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
decimalShift
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#15) is not in mixedCase
Parameter
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
bridgeOnOtherSide
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#16) is not in mixedCase
Parameter ForeignBridgeErcToNative.claimTokens(address,address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#45) is not in mixedCase
```



```
Parameter ForeignBridgeErcToNative.claimTokens(address,address)._to
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#45) is not in mixedCase
Parameter ForeignBridgeErcToNative.onExecuteMessage(address,uint256,bytes32)._recipient
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#52) is not in mixedCase
Parameter ForeignBridgeErcToNative.onExecuteMessage(address,uint256,bytes32)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#53) is not in mixedCase
Parameter ForeignBridgeErcToNative.relayTokens(address,uint256)._receiver
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#64) is not in mixedCase
Parameter ForeignBridgeErcToNative.relayTokens(address,uint256)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#64) is not in mixedCase
Parameter InterestConnector.isInterestEnabled(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#39) is not in mixedCase
Parameter InterestConnector.initializeInterest(address,uint256,uint256,address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#51) is not in mixedCase
Parameter InterestConnector.initializeInterest(address,uint256,uint256,address)._minCashThreshold
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#52) is not in mixedCase
Parameter InterestConnector.initializeInterest(address,uint256,uint256,address)._minInterestPaid
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#53) is not in mixedCase
Parameter InterestConnector.initializeInterest(address,uint256,uint256,address)._interestReceiver
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#54) is not in mixedCase
Parameter InterestConnector.setMinCashThreshold(address,uint256)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#71) is not in mixedCase
Parameter InterestConnector.setMinCashThreshold(address,uint256)._minCashThreshold
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#71) is not in mixedCase
Parameter InterestConnector.minCashThreshold(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#80) is not in mixedCase
Parameter InterestConnector.setMinInterestPaid(address,uint256)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#90) is not in mixedCase
Parameter InterestConnector.setMinInterestPaid(address,uint256)._minInterestPaid
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#90) is not in mixedCase
Parameter InterestConnector.minInterestPaid(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#99) is not in mixedCase
Parameter InterestConnector.disableInterest(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#108) is not in mixedCase
Parameter InterestConnector.interestReceiver(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#118) is not in mixedCase
```

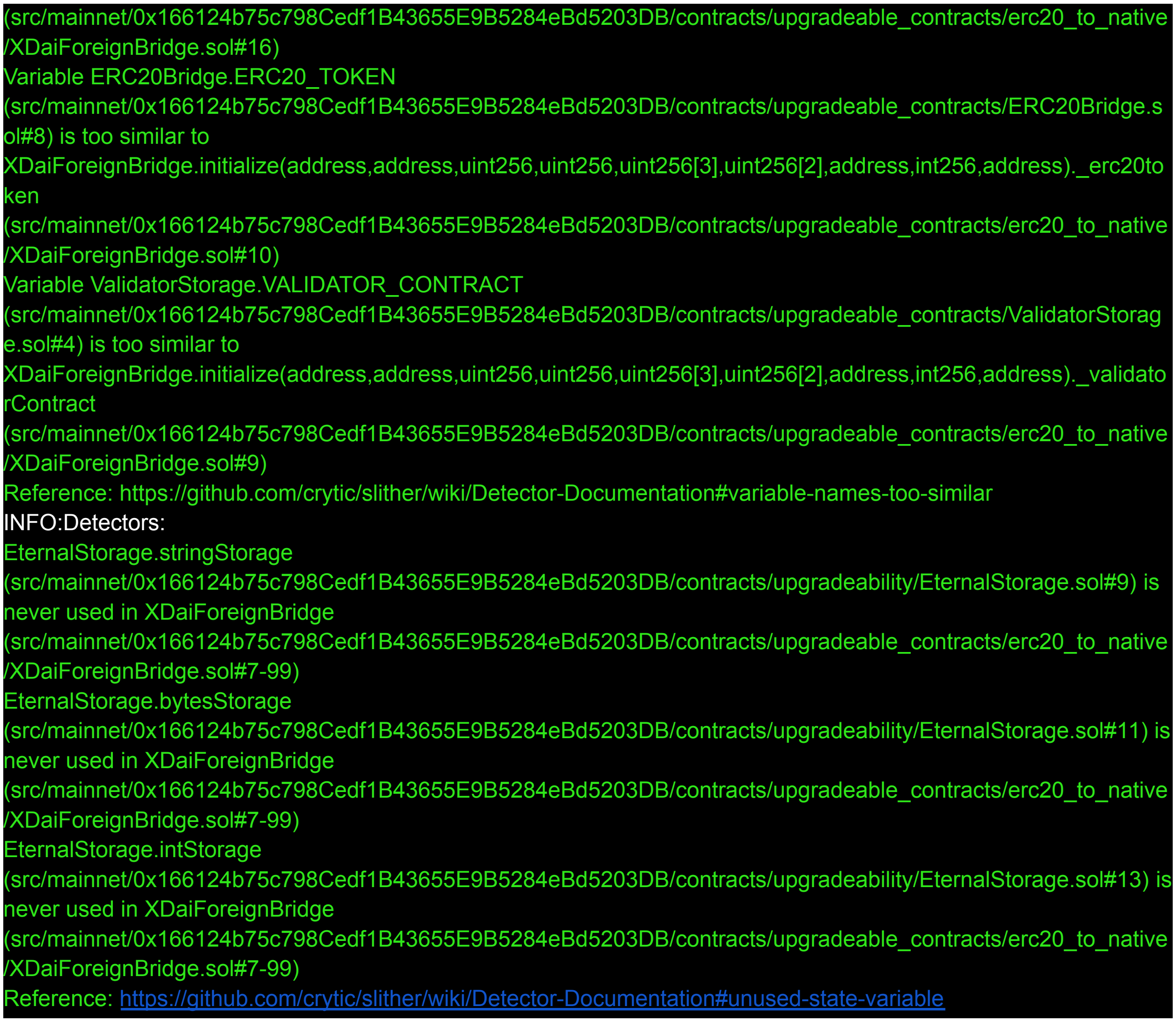


```
Parameter InterestConnector.setInterestReceiver(address,address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#128) is not in mixedCase
Parameter InterestConnector.setInterestReceiver(address,address)._receiver
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#128) is not in mixedCase
Parameter InterestConnector.payInterest(address,uint256)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#138) is not in mixedCase
Parameter InterestConnector.payInterest(address,uint256)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#138) is not in mixedCase
Parameter InterestConnector.investedAmount(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#155) is not in mixedCase
Parameter InterestConnector.invest(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/InterestConnector.sol#164) is not in mixedCase
Parameter SavingsDaiConnector.interestAmount(address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/SavingsDaiConnector.sol#32) is not in mixedCase
Parameter SavingsDaiConnector.previewWithdraw(address,uint256)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/SavingsDaiConnector.sol#78) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._validato
rContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#9) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._erc20to
ken
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#10) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._required
BlockConfirmations
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#11) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._gasPric
e
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#12) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._dailyLim
itMaxPerTxMinPerTxArray
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#13) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._homeD
ailyLimitHomeMaxPerTxArray
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#14) is not in mixedCase
```



```
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._owner
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#15) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._decimal
Shift
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#16) is not in mixedCase
Parameter
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._bridgeO
nOtherSide
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#17) is not in mixedCase
Parameter XDaiForeignBridge.claimTokens(address,address)._token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#64) is not in mixedCase
Parameter XDaiForeignBridge.claimTokens(address,address)._to
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#64) is not in mixedCase
Parameter XDaiForeignBridge.onExecuteMessage(address,uint256,bytes32)._recipient
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#73) is not in mixedCase
Parameter XDaiForeignBridge.onExecuteMessage(address,uint256,bytes32)._amount
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#74) is not in mixedCase
Parameter SafeMath.mul(uint256,uint256)._a
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#13) is not in mixedCase
Parameter SafeMath.mul(uint256,uint256)._b
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#13) is not in mixedCase
Parameter SafeMath.div(uint256,uint256)._a
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#29) is not in mixedCase
Parameter SafeMath.div(uint256,uint256)._b
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#29) is not in mixedCase
Parameter SafeMath.sub(uint256,uint256)._a
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#39) is not in mixedCase
Parameter SafeMath.sub(uint256,uint256)._b
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#39) is not in mixedCase
Parameter SafeMath.add(uint256,uint256)._a
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#47) is not in mixedCase
Parameter SafeMath.add(uint256,uint256)._b
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/node_modules/openzeppelin-solidity/contracts/m
ath/SafeMath.sol#47) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Function CounterTest.test_Increment() (test/Counter.t.sol#15-18) is not in mixedCase
Function CounterTest.testFuzz_SetNumber(uint256) (test/Counter.t.sol#20-23) is not in mixedCase
```

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable BasicTokenBridge.DAILY_LIMIT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#16) is too similar to BasicTokenBridge.maxAvailablePerTx()._dailyLimit
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#103)
Variable BasicTokenBridge.DAILY_LIMIT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#16) is too similar to BasicTokenBridge.setExecutionDailyLimit(uint256)._dailyLimit
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#76)
Variable BasicTokenBridge.DAILY_LIMIT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#16) is too similar to BasicTokenBridge.setDailyLimit(uint256)._dailyLimit
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/BasicTokenBrid
ge.sol#70)
Variable GSNForeignERC20Bridge.TRUSTED_FORWARDER
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#10) is too similar to GSNForeignERC20Bridge.setTrustedForwarder(address)._trustedForwarder
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/GSNForeignER
C20Bridge.sol#20)
Variable OtherSideBridgeStorage.BRIDGE_CONTRACT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/OtherSideBridg
eStorage.sol#6) is too similar to OtherSideBridgeStorage._setBridgeContractOnOtherSide(address)._bridgeContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/OtherSideBridg
eStorage.sol#8)
Variable ERC20Bridge.ERC20_TOKEN
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#8) is too similar to
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
erc20token
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#9)
Variable ValidatorStorage.VALIDATOR_CONTRACT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ValidatorStorag
e.sol#4) is too similar to
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
validatorContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#8)
Variable DecimalShiftBridge.DECIMAL_SHIFT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#9) is too similar to
ForeignBridgeErcToNative.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._
decimalShift
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/ForeignBridgeErcToNative.sol#15)
Variable DecimalShiftBridge.DECIMAL_SHIFT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/DecimalShiftBri
dge.sol#9) is too similar to
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._decimal
Shift
```



```
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#16)
Variable ERC20Bridge.ERC20_TOKEN
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ERC20Bridge.s
ol#8) is too similar to
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._erc20to
ken
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#10)
Variable ValidatorStorage.VALIDATOR_CONTRACT
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/ValidatorStorag
e.sol#4) is too similar to
XDaiForeignBridge.initialize(address,address,uint256,uint256,uint256[3],uint256[2],address,int256,address)._validato
rContract
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#9)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
EternalStorage.stringStorage
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeability/EternalStorage.sol#9) is
never used in XDaiForeignBridge
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#7-99)
EternalStorage.bytesStorage
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeability/EternalStorage.sol#11) is
never used in XDaiForeignBridge
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#7-99)
EternalStorage.intStorage
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeability/EternalStorage.sol#13) is
never used in XDaiForeignBridge
(src/mainnet/0x166124b75c798Cedf1B43655E9B5284eBd5203DB/contracts/upgradeable_contracts/erc20_to_native
/XDaiForeignBridge.sol#7-99)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable
```

Results

Apart from unchecked transfers, no major issues were discovered. Some false positive errors were flagged by the tool. All remaining issues have been diligently categorized and documented in the GitHub repository file named `AutomatedToolFindings.md`.

Closing Summary

Overall, the smart contracts are meticulously crafted. While several issues were uncovered during the audit process, with high severity issues a few and, most other issues are medium and low level issues, AutomatedToolFindings.md it is advised to the team to effectively address the majority of these concerns, ensuring the integrity and robustness of the contracts.