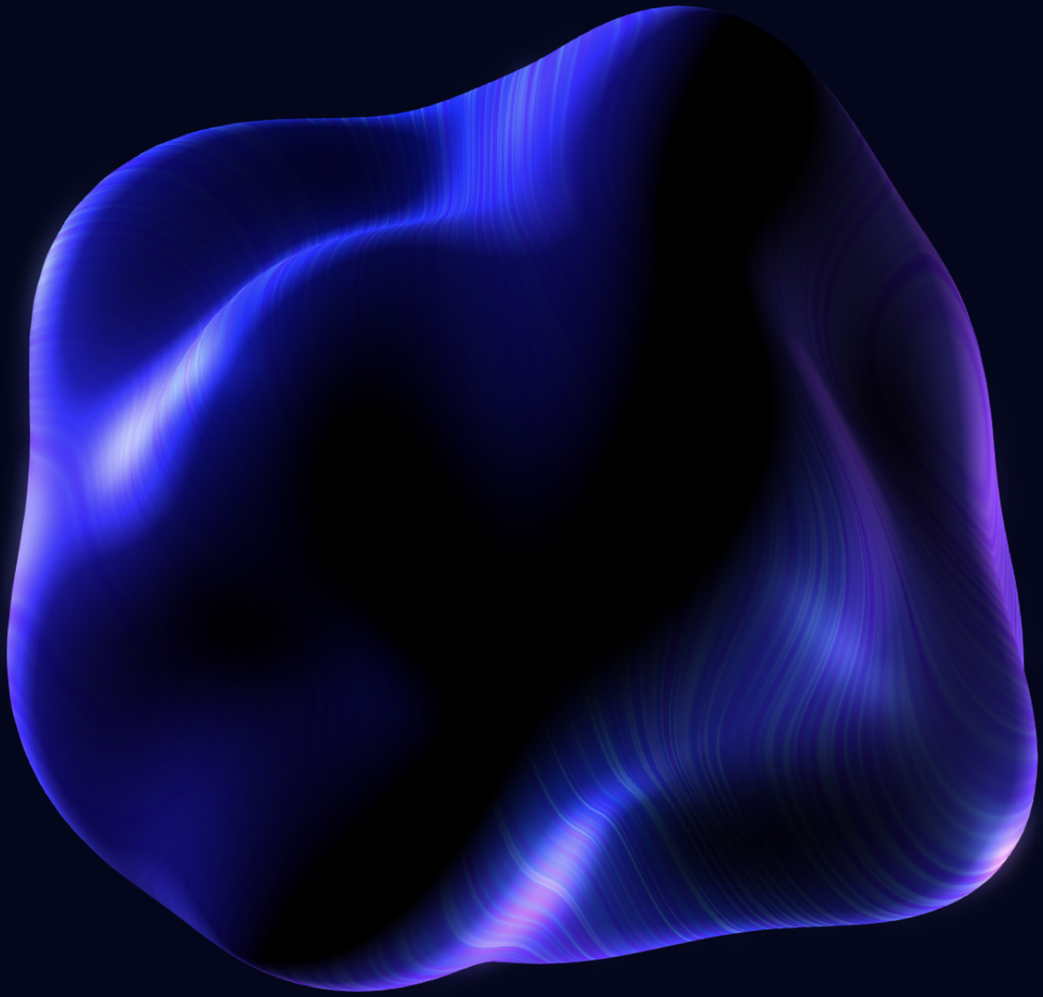
MUNDUS SECURITY

Insured Security Smart Contract Audit of Safe on zkSync

Verification of Fixes & Deployment Performed by Protofire



Insured by Atomica.org

atomica™

🌐 mundus.dev

@mundus_security

Mundus.dev

MUNDUS
SECURITY

Protofire zkSync Safe deployment check and security audit

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.
The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

Scope of work

Contract	address
SimulateTxAccessor	0xD7C05A08cB43e99d596B606A1c03EA2F21289d94
GnosisSafeProxyFactory	0x07551c0Daf6fCD9bc2A398357E5C92C139724Ef3
DefaultCallbackHandler	0x9efc6C710c6C616A99A1769c0579c9a1c71B0bcA
CompatibilityFallbackHandler	0x951CdaE973fc2c312456238Fb1f96e5b4FF6638c
CreateCall	0xD03e9f3Ff5feE3A1Ef06f806504efF40A4f3967a
MultiSend	0x4Cf127E857086851359BA9Ec60F66B43887CEa52
MultiSendCallOnly	0xeB764c4Be80FE1842bd328622E699bF919500D57
SignMessageLib	0x06DF6D795B81a47c77c2f6570F4e1f34eb9070D6
GnosisSafeL2	0x439540E330eA6e28d73729eDc5C83578d3d3dFde
GnosisSafe	0xbDEf90f0b9023eD929f885FAf81b4d7b89165B6a

Reference information

Name	Protofire zkSync Safe
Website	https://safe.protofire.io/
Language	Solidity
Chain	zkSync Era testnet
Reference repository	https://github.com/safe-global/safe-contracts
Reference release	v1.3.0-libs.0 767ef36bba88bdbc0c9fe3708a4290cabef4c376
Audit of reference release	G0 Group audit
Reference deployments	https://github.com/safe-global/safe-deployments/tree/main/src/assets/v1.3.0 chainId: 1 (ethereum)

Table of contents

Findings summary

Deployment check

Contract	Source code issues	Storage issues
SimulateTxAccessor	none	none
GnosisSafeProxyFactory	found	none
DefaultCallbackHandler	none	none
CompatibilityFallbackHandler	none	none
CreateCall	none	none
MultiSend	none	none
MultiSendCallOnly	none	none
SignMessageLib	none	none
GnosisSafeL2	none	none
GnosisSafe	none	none

Source code audit

Severity	Number
Informational	1

Deployment check

SimulateTxAccessor

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

None

Unstructured Storage

None

GnosisSafeProxyFactory

Source code

Differences with the reference code base are described in the Source code audit section.

Structured Storage

name	type	slot	value	coincides with reference
singleton	address	0	0x0	true

Unstructured Storage

None

DefaultCallbackHandler

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

None

Unstructured Storage

None

CompatibilityFallbackHandler

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

name	type	slot	value	coincides with reference
approvedHashes	mapping	8	0x0	true
signedMessages	mapping	7	0x0	true
_deprecatedDomainSeparator	bytes32	6	0x0	true
nonce	uint256	5	0	true
threshold	uint256	4	0	true
ownerCount	uint256	3	0	true
owners	mapping	2	0x0	true
modules	mapping	1	0x0	true
singleton	address	0	0x0	true

Unstructured Storage

name	slot	value	coincides with reference
GUARD_STORAGE_SLOT	0x4a204...c34c8	0x0	true
FALLBACK_HANDLER_STORAGE_SLOT	0x6c9a6...918d5	0x0	true

CreateCall

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

None

Unstructured Storage

None

MultiSend

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

None

Unstructured Storage

None

MultiSendCallOnly

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

None

Unstructured Storage

None

SignMessageLib

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

name	type	slot	value	coincides with reference
approvedHashes	mapping	8	0x0	true
signedMessages	mapping	7	0x0	true
_deprecatedDomainSeparator	bytes32	6	0x0	true
nonce	uint256	5	0	true
threshold	uint256	4	0	true
ownerCount	uint256	3	0	true
owners	mapping	2	0x0	true
modules	mapping	1	0x0	true
singleton	address	0	0x0	true

Unstructured Storage

name	slot	value	coincides with reference
GUARD_STORAGE_SLOT	0x4a204...c34c8	0x0	true
FALLBACK_HANDLER_STORAGE_SLOT	0x6c9a6...918d5	0x0	true

GnosisSafeL2

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

name	type	slot	value	coincides with reference
approvedHashes	mapping	8	0x0	true
signedMessages	mapping	7	0x0	true
_deprecatedDomainSeparator	bytes32	6	0x0	true
nonce	uint256	5	0	true
threshold	uint256	4	1	true
ownerCount	uint256	3	0	true
owners	mapping	2	0x0	true
modules	mapping	1	0x0	true
singleton	address	0	0x0	true

Unstructured Storage

name	slot	value	coincides with reference
GUARD_STORAGE_SLOT	0x4a204...c34c8	0x0	true
FALLBACK_HANDLER_STORAGE_SLOT	0x6c9a6...918d5	0x0	true

GnosisSafe

Source code

The deployed source code including all imports and transitive imports matches the reference version.

Structured Storage

name	type	slot	value	coincides with reference
approvedHashes	mapping	8	0x0	true
signedMessages	mapping	7	0x0	true
_deprecatedDomainSeparator	bytes32	6	0x0	true
nonce	uint256	5	0	true
threshold	uint256	4	1	true
ownerCount	uint256	3	0	true
owners	mapping	2	0x0	true
modules	mapping	1	0x0	true
singleton	address	0	0x0	true

Unstructured Storage

name	slot	value	coincides with reference
GUARD_STORAGE_SLOT	0x4a204...c34c8	0x0	true
FALLBACK_HANDLER_STORAGE_SLOT	0x6c9a6...918d5	0x0	true

Source code audit

The source code for all smart contracts under SoW matches reference code base, which was audited by G0 Group, except the following list of differences:

1. Informational: proxyRuntimeCode method removed GnosisSafeProxyFactory

The proxyRuntimeCode method is removed from the GnosisSafeProxyFactory contract to facilitate the project deployment to zkSync Era chain. This is a safe change, as the proxyRuntimeCode method is not used by any other smart contract in the project and, thus, is not able to affect the logic of the protocol.

```
/* function proxyRuntimeCode() public pure returns (bytes memory) {
    return type(GnosisSafeProxy).runtimeCode;
} */
```

Disclaimers

Mundus disclaimer

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

Technical disclaimers

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.