DeHacker

Code Security Assessment

Axelarnetwork

July 29th, 2022

Contents

Summary

DeHacker's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.
Possible issues we looked for included (but are not limited to):

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire code base by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes.
- Add enough unit tests to cover the possible use cases.
- Provide more comments per each function for readability, especially contracts that are verified in public.
- Provide more transparency on privileged activities once the protocol is live.

Issue Categories

Every issue in this report was assigned a severity level from the following:

Critical severity issues

A vulnerability that can disrupt the contract functioning in a number of scenarios or creates a risk that the contract may be broken.

Major severity issues

A vulnerability that affects the desired outcome when using a contract or provides the opportunity to use a contract in an unintended way.

Medium severity issues

A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.

Minor severity issues

A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.

Informational

A vulnerability that has informational character but is not affecting any of the code.

Overview

Project Summary

Project Name	Axelarnetwork
Platform	Ethereum
website	https://trustwallet.com/
Type	Others
Deployed contract	https://github.com/axelarnetwork/solidity-cgp-gateway
Language	Solidity

Audit Summary

Delivery Date	July 29th 2022
Audit Methodology	Static Analysis, Manual Review

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	0	0	0	0	0	0
Medium	1	0	0	0	0	1
Minor	0	0	0	0	0	0
Informational	0	0	0	3	0	0
Discussion	0	0	0	0	0	0

Audit scope

ID	File	SHA256 Checksum
AGM	AxelarNetwork/contracts/AxelarGatewayMultisig.sol	2c669ac6b63ff27c4e037295949a90af9c93dbabc52679d6e5f9a41550ea6085
IER	AxelarNetwork/contracts/interfaces/IERC20.sol	32a03a4f2c670cf3868650db4d33d12510c4b23d2ed210c7fbe87010a9cea5df
AGS	AxelarNetwork/contracts/AxelarGatewaySinglesig.sol	d0adc702e0dbddad1078fdbe24be0df1664e2ad2a3c961067f2fb0105a4f76be
ANK	AxelarNetwork/contracts/util	
AGA	AxelarNetwork/contracts/AxelarGateway.sol	b939479c0adc00d513cfc0e4a831e85d69c94c8d99f6cc1d8570800cebf2f3d3
CAN	AxelarNetwork/contracts/Context.sol	74822d543f5485c90607cd393ed0a51379adeb97a4365315bca3aef6131a010f
AFA	AxelarNetwork/contracts/util/AddressFormat.sol	b0a6c4ec792e93ef12f4d8ed447224018f9ba98cd21b9d1df690d7e23d946fb1

ESA	AxelarNetwork/contracts/ EternalStorage.sol	
IAS	AxelarNetwork/contracts/interfaces/ IAxelarGatewaySinglesig.sol	2b6582375d61ddd6e37a234a19b1921df2e2ad29709b384ffd162b 7cdbbabcb5
ANC	AxelarNetwork/contracts/ interfaces	
IAM	AxelarNetwork/contracts/interfaces/ IAxelarGatewayMultisig.sol	520bbafa346817594ebb661fe515142e4bcddc3b862718a9eb9aa a2226cc965e
DHA	AxelarNetwork/contracts/ DepositHandler.sol	e1de312c21bbbb0c087972e1d1d581069d2f1083a35f8f14418ac6 01abf0d487
IEC	AxelarNetwork/contracts/ interfaces/IERC20BurnFrom.sol	1e3162d6cc4e51903fc5f0484e7611dca973d74425b0a3a7027d0d f59771de96
TDA	AxelarNetwork/contracts/ TokenDeployer.sol	3392ead2485c8deac3e5fbf296b6e1f08c48a6f26804069b7e01b9 3df30deb07
ERP	AxelarNetwork/contracts/ ERC20Permit.sol	6639079c2a6ebf8128cd6ff47821f6931ac35dfd54580084807b8733 33f12561
AMB	AxelarNetwork/contracts/ AdminMultisigBase.sol	4bbf10c558f953bff3536d0d88d69c712b249968715ed43d8ea7e9 c4b1a5cfde
OAN	AxelarNetwork/contracts/ Ownable.sol	d069d2a157af014f7a218fda322b12ec6ee42ca5c1ce304f0882f2c ccd0589fb
MCE	AxelarNetwork/contracts/ MintableCappedERC20.sol	6866b32898fd047b78012abe0ba8cffa17c7b30234552c5eb1535b 8eabb5ac82
IAE	AxelarNetwork/contracts/ interfaces/IAxelarExecutable.sol	eda71300473f064ae00772ecc890da9e3b23a77a6260493fb7a74 520c1e2d1d1
BMC	AxelarNetwork/contracts/ interfaces/IAxelarExecutable.sol	d0adc702e0dbddad1078fdbe24be0df1664e2ad2a3c961067f2fb 0105a4f76be
ECD	AxelarNetwork/contracts/ ECDSA.sol	d55489743abf362b026b9904bf42ef3af56066907dc7490a1514e66 45ae8089c
IAG	AxelarNetwork/contracts/ interfaces/IAxelarGateway.sol	55d779d46a44d5d61f9107d043d3cd858fcc6756b15a5639a906b5 b8b108a398
ERC	AxelarNetwork/contracts/ ERC20.sol	f381288a2d30096e193233269a3662884babf26fd1ecf1dd209c7fe d1bb20a2c
AGP	AxelarNetwork/contracts/ AxelarGatewayProxy.sol	b229ce5feaab0a356607c8c4bf1ba2f0aea29254a959d0b5c76f8 3296e996741

Findings

ID	Title	Category	Severity	Status
AGA-01	freezeToken Doesn't AffectTokenType.External Tokens	Logical Issue	Medium	Resolved
AGA-02	It's Better To Set A Time Delay	Logical Issue	Informational	Acknowledged
AGA-03	TokenType.InternalBurnable Token Doesn'tExist	Logical Issue	Informational	Acknowledged
AGM-01	It's Better To Set A Min Threshold	Logical Issue	Informational	Acknowledged

Medium

AGA-01 | freezeToken Doesn't Affect TokenType.External Tokens

Category	Severity	Location	Status
Logical Issue	Medium	AxelarNetwork/ contracts/ AxelarGateway. sol: 229, 336	Resolved

Description

If the KEY_ALL_TOKENS_FROZEN value is true or a TokenType.External token is frozen, the function_burnTokenFrom and _mintToken can still be called successfully, but other types of tokens will be failed.

Recommendation

We recommend fixing this logic issue.

Alleviation

Fixed in commit 4067ed6c8f7e8d5d09d94d6b7301919aff2cb8fc .

Informational

AGA-02 | It's Better To Set A Time Delay

Category	Severity	Location	Status
Logical Issue	Informational	AxelarNetwork/ contracts/ AxelarGateway. sol: 203	Acknowledged

Description

The function upgrade can upgrade the implementation of the contract; although it is managed by multiadmins, it's better to add a time delay when upgrading the contract.

Recommendation

We recommend adding a time delay of at least 48 hours to upgrade the contract.

Informational

AGA-03 | TokenType.InternalBurnable Token Doesn't Exist

Category	Severity	Location	Status
Logical Issue	Medium	AxelarNetwork/ contracts/ AxelarGateway. sol: 264~276	Acknowledged

Description

TokenType.InternalBurnable tokens are not deployed in this contract.

Recommendation

We advise explaining to users.

Alleviation

[Axelar Network] InternalBurnable token type is purely around for backwards compatibility for tokensthat were deployed in v1.0.0 of the contracts.

Informational

AGM-01 | It's Better To Set A Min Threshold

Category	Severity	Location	Status
Logical Issue	Informational	AxelarNetwork/ contracts/ AxelarGatewayMultisig.sol: 401, 413, 435, 439, 443	Acknowledged

Description

In the setup function, the valid min threshold(adminThreshold / ownerThreshold / operatorThreshold) is1 ; because it's multi-sign, it's better to set a multi number like 3 .

Recommendation

We recommend adding validation to ensure the minimum threshold is at least three.

Alleviation

[Axelar Network] Allowing the threshold to be 1 allows support for single sig easily (threshold signatures)in the future with the same contract. Also, the contracts are not made more restrictive than the networkitself to avoid a state mismatch between the gateway and the network.

Disclaimer

This report is subject to the terms and conditions (including but not limited to the description of the Services, confidentiality, disclaimers and limitations of liability) or scope of the Services set forth in the Service Agreement and the terms and conditions provided to you (the "Customer" or the "Company") in connection with this Agreement. This report relating to the Services set forth herein shall be used by the Company only to the extent permitted by the terms and conditions set forth herein. No one may transmit, disclose, quote or rely on this report for any purpose, nor may a copy be delivered to any person other than the Company, without Dehacker' prior written consent.

This report is not and should not be construed as an "endorsement" or "disapproval" of any particular project or team. This report is not and should not be construed as an indication of the economics or value of any product or asset created by any team or program contracted by Dehacker for the safety assessment. This report does not provide any warranties or warranties as to the absolutely defect-free nature of the analyzed technology, nor does it provide any indication of the technology owner, business, business model, or legal compliance.

This report should not be used in any way to make decisions surrounding investment or participation in any particular project. This report in no way provides investment advice and should not be used as investment advice of any kind. This report represents a broad evaluation process designed to help our customers improve the quality of their code while reducing the high risks posed by cryptographic tokens and blockchain technology.

Blockchain technology and crypto assets have a high level of ongoing risk. Dehacker' position is that each company and individual is responsible for their own due diligence and ongoing safety. The goal of Dehacker is to help reduce the medium of attack and the high level of variance associated with utilizing new and changing technologies, and in no way guarantee the safety or functionality of the technologies we agree to analyze.

The assessment service provided by Dehacker is influenced by dependencies and is under continued development. You agree that your access and/or use, including but not limited to any services, reports and materials, will be at your own risk as is, as is and as available. Cryptographic tokens are an emerging technology and carry a high level of technical risk and uncertainty. Evaluation reports may include false positives, false negatives, and other unpredictable results. These services can access and rely on multiple layers of third parties.

ALL SERVICES, LABELS, EVALUATION REPORTS, WORK PRODUCTS OR OTHER MATERIALS, OR ANY PRODUCT OR USE RESULTS ARE PROVIDED "AS IS" AND "AVAILABLE" WITHOUT WARRANTIES OF ANY KIND FOR FAULTS AND DEFECTS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, Dehacker DISCLAIMS ANY

WARRANTY, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, FOR THE SERVICES, EVALUATION REPORTS OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, DehackerS EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE TRANSACTION, USE OR TRADE PRACTICES. WITHOUT LIMITING THE FOREGOING, Dehacker DON'T GUARANTEE SERVICE, TAG, ASSESSMENT, WORK PRODUCTS, OR OTHER MATERIAL, OR THE USE OF ANY PRODUCT OR RESULT WILL MEET THE REQUIREMENTS OF CUSTOMERS OR ANY OTHERS, REALIZATION OF THE EXPECTED RESULTS OF ANY COMPATIBLE WITH ANY SOFTWARE, SYSTEM OR OTHER SERVICES, OR SAFE, ACCURATE AND COMPLETE, NO HARMFUL CODE OR NO ERROR. WITHOUT LIMITING THE FOREGOING, Dehacker DOESN'T PROVIDE ANY GUARANTEE OR PROMISE, ALSO DO NOT MAKE ANY STATEMENT, AS A SERVICE TO MEET THE REQUIREMENTS OF CUSTOMERS, IMPLEMENT ANY EXPECTED RESULTS, AND ANY OTHER SOFTWARE, APPLICATION, SYSTEM OR SERVICE COMPATIBLE OR WORK TOGETHER, CONTINUOUS OPERATION, TO MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR ERROR-FREE, OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER Dehacker NOR ANY Dehacker AGENT MAKES ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, RELIABILITY OR TIMELINESS OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICES. Dehacker SHALL NOT BE LIABLE OR LIABLE FOR ANY ERRORS, ERRORS OR INACCURACIES IN THE CONTENT AND MATERIALS, OR FOR ANY LOSS OR DAMAGE OF ANY KIND ARISING OUT OF THE USE OF ANY CONTENT, OR (II) FOR PERSONAL INJURY OR PROPERTY DAMAGE OF ANY NATURE ARISING OUT OF CUSTOMER'S ACCESS TO OR USE OF THE SERVICES. EVALUATION REPORT OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATIONS OR WARRANTIES OF ANY THIRD-PARTY MATERIALS OR RELATING TO ANY THIRD-PARTY MATERIALS ARE STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNERS OR DISTRIBUTORS OF THE THIRD-PARTY MATERIALS.

THE SERVICES, EVALUATION REPORTS AND ANY OTHER MATERIALS UNDER THIS AGREEMENT ARE PROVIDED TO THE CUSTOMER ONLY AND SHALL NOT BE RELIED UPON BY ANY COMPANY

COPIES MAY NOT BE DELIVERED TO ANY OTHER PERSON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT EXPRESSLY SPECIFIED IN THIS AGREEMENT WITHOUT Dehacker 'PRIOR WRITTEN CONSENT.

NO THIRD PARTY OR ANY PERSON ACTING ON BEHALF OF ANY THIRD PARTY SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, EVALUATION REPORTS AND ANY ACCOMPANYING MATERIALS, AND NO SUCH THIRD PARTY SHALL BE ENTITLED TO MAKE ANY CONTRIBUTION TO Dehacker WITH RESPECT TO SUCH SERVICES, EVALUATION REPORTS AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF Dehacker CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF THE CUSTOMER. THEREFORE, NO THIRD PARTY OR ANY PERSON

ACTING ON BEHALF OF ANY SUCH REPRESENTATIONS AND WARRANTIES SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES, AND NO SUCH THIRD PARTY SHALL BE ENTITLED TO MAKE ANY CONTRIBUTION TO Dehacker WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER THAT IS BOUND BY THIS AGREEMENT OR OTHERWISE OR WHICH GIVES RISE TO INDEMNIFICATION.

FOR THE AVOIDANCE OF DOUBT, THE SERVICES (INCLUDING ANY RELATED EVALUATION REPORTS OR MATERIALS) SHOULD NOT BE REGARDED OR RELIED UPON FOR FINANCIAL, TAX, LEGAL, REGULATORY OR OTHER ADVICE OF ANY KIND.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Coding Style

Coding Style findings usually do not affect the generated bytecode but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block. timestamp works.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux “sha256sum" command against the target file.

About

DeHacker is a team of auditors and white hat hackers who perform security audits and assessments. With decades of experience in security and distributed systems, our experts focus on the ins and outs of system security. Our services follow clear and prudent industry standards. Whether it's reviewing the smallest modifications or a new platform, we'll provide an in-depth security survey at every stage of your company's project. We provide comprehensive vulnerability reports and identify structural inefficiencies in smart contract code, combining high-end security research with a real-world attacker mindset to reduce risk and harden code.

BLOCKCHAIINS

Ethereum

Cosmos

Eos

Substrate

TECH STACK

Python

Solidity

Rust

c++

CONTACTS

https://dehacker.io

https://twitter.com/dehackerio

https://github.com/dehacker/audits_public

https://t.me/dehackerio

https://blog.dehacker.io/

audit@dehacker.io

DeHacker

July 2022