CERTIK

Security Assessment

Axelarnetwork

Apr 22nd, 2022

Table of Contents

Summary

This report has been prepared for Axelarnetwork to discover issues and vulnerabilities in the source code of the Axelarnetwork project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- 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 codebase 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.

Overview

Project Summary

Project Name	Axelarnetwork
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/axelarnetwork/solidity-cgp-gateway
Commit	

Audit Summary

Delivery Date	Apr 22, 2022 UTC
Audit Methodology	Static Analysis, Manual Review

Vulnerability Summary

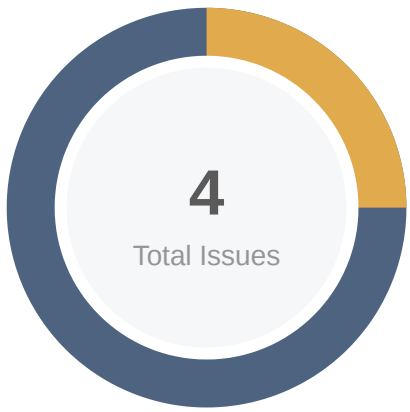
Vulnerability Level	Total	Pending	Declined	Acknowledged	Mitigated	Partially Resolved	Resolved
Critical	0	0	0	0	0	0	0
Major	0	0	0	0	0	0	0
Medium	1	0	0	0	0	0	1
Minor	0	0	0	0	0	0	0
Informational	3	0	0	3	0	0	0
Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
AGM	AxelarNetwork/contracts/AxelarGatewayMultisig.sol	2c669ac6b63ff27c4e037295949a90af9c93dbabc52679d6e5f9a41550ea6085
IER	AxelarNetwork/contracts/interfaces/IERC20.sol	32a03a4f2c670cf3868650db4d33d12510c4b23d2ed210c7fbe87010a9cea5df
AGS	AxelarNetwork/contracts/AxelarGatewaySinglesig.sol	024460b984c81a8651e2b0fcafba8d803fe4cd8e5f926f93a74bac4d118ed196
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	c27a1ecacaf28715baf068147b770ffbdf612f4b44dfe5c3067d43341e08bea1
IAS	AxelarNetwork/contracts/interfaces/IAxelarGatewaySinglesig.sol	2b6582375d61ddd6e37a234a19b1921df2e2ad29709b384ffd162b7cdbbabcb5
ANC	AxelarNetwork/contracts/interfaces	
IAM	AxelarNetwork/contracts/interfaces/IAxelarGatewayMultisig.sol	520bbafa346817594ebb661fe515142e4bcddc3b862718a9eb9aaa2226cc965e
DHA	AxelarNetwork/contracts/DepositHandler.sol	e1de312c21bbbb0c087972e1d1d581069d2f1083a35f8f14418ac601abf0d487
IEC	AxelarNetwork/contracts/interfaces/IERC20BurnFrom.sol	1e3162d6cc4e51903fc5f0484e7611dca973d74425b0a3a7027d0df59771de96
TDA	AxelarNetwork/contracts/TokenDeployer.sol	3392ead2485c8deac3e5fbf296b6e1f08c48a6f26804069b7e01b93df30deb07
ERP	AxelarNetwork/contracts/ERC20Permit.sol	6639079c2a6ebf8128cd6ff47821f6931ac35dfd54580084807b873333f12561
AMB	AxelarNetwork/contracts/AdminMultisigBase.sol	4bbf10c558f953bff3536d0d88d69c712b249968715ed43d8ea7e9c4b1a5cfde

ID	File	SHA256 Checksum
OAN	AxelarNetwork/contracts/Ownable.sol	d069d2a157af014f7a218fda322b12ec6ee42ca5c1ce304f0882f2cccd0589fb
MCE	AxelarNetwork/contracts/MintableCappedERC20.sol	6866b32898fd047b78012abe0ba8cffa17c7b30234552c5eb1535b8eabb5ac82
IAE	AxelarNetwork/contracts/interfaces/IAxelarExecutable.sol	eda71300473f064ae00772ecc890da9e3b23a77a6260493fb7a74520c1e2d1d1
BMC	AxelarNetwork/contracts/BurnableMintableCappedERC20.sol	266b8b5301786d2f2671c14a029b4e322f586e4649a3cc2f0891520bfb54fc8d
ECD	AxelarNetwork/contracts/ECDSA.sol	d55489743abf362b026b9904bf42ef3af56066907dc7490a1514e6645ae8089c
IAG	AxelarNetwork/contracts/interfaces/IAxelarGateway.sol	55d779d46a44d5d61f9107d043d3cd858fcc6756b15a5639a906b5b8b108a398
ERC	AxelarNetwork/contracts/ERC20.sol	f381288a2d30096e193233269a3662884babf26fd1ecf1dd209c7fed1bb20a2c
AGP	AxelarNetwork/contracts/AxelarGatewayProxy.sol	b229ce5feaab0a356607c8c4bf1ba2f0aea29254a959d0b5c76f83296e996741

Findings



Critical	**0** (0.00%)
Major	**0** (0.00%)
Medium	**1** (25.00%)
Minor	**0** (0.00%)
Informational	**3** (75.00%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
AGA-01	`freezeToken` Doesn't Affect `TokenType.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't Exist	Logical Issue	Informational	Acknowledged
AGM-01	It's Better To Set A Min Threshold	Logical Issue	Informational	Acknowledged

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`.

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 multi admins, 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.

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

Category	Severity	Location	Status
Logical Issue	Informational	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 tokens that were deployed in `v1.0.0` of the contracts.

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`) is `1`; 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 network itself to avoid a state mismatch between the gateway and the network.

Appendix

Finding Categories

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.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND

“AS AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER’S OR ANY OTHER PERSON’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK’S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER’S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED “AS IS” AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK’S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.