

MatterLabs -Verifier

Smart Contract Security Assessment

Prepared by: Halborn

Date of Engagement: July 12th, 2023 - July 20th, 2023

Visit: Halborn.com

DOCU	MENT REVISION HISTORY	2
CONT	ACTS	2
1	EXECUTIVE OVERVIEW	3
1.1	INTRODUCTION	4
1.2	ASSESSMENT SUMMARY	4
1.3	SCOPE	5
1.4	TEST APPROACH & METHODOLOGY	6
2	RISK METHODOLOGY	7
2.1	EXPLOITABILITY	8
2.2	IMPACT	9
2.3	SEVERITY COEFFICIENT	11
3	ASSESSMENT SUMMARY & FINDINGS OVERVIEW	13
4	MANUAL TESTING	13
5	AUTOMATED TESTING	24
5.1	STATIC ANALYSIS REPORT	25
	Description	25
	Slither results	25
5.2	AUTOMATED SECURITY SCAN	27
	Description	27
	MythX results	27

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Draft Document	07/21/2023	Gabi Urrutia
1.0	Final Report	09/15/2023	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

This assessment was entirely focused on the new version of zkSync verifier which is a modified version of the Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge (PLONK) to optimize the proof system for zkSync Era circuits.

MatterLabs engaged Halborn to conduct a security assessment on their verifier smart contract beginning on July 12th, 2023 and ending on July 20th, 2023. The security assessment was scoped to the smart contract provided to the Halborn team.

1.2 ASSESSMENT SUMMARY

The team at Halborn was provided one week for the engagement and assigned a full-time security engineer to verify the security of the smart contract. The security engineer is a blockchain and smart-contract security expert with advanced penetration testing, smart-contract hacking, and deep knowledge of multiple blockchain protocols.

The purpose of this assessment is to:

- Ensure that smart contract functions operate as intended
- Identify potential security issues within the smart contract

In summary, Halborn did not identify any security risks within the verifier smart contract.

1.3 SCOPE

1. IN-SCOPE:

The security assessment was scoped to the following smart contract:

• ethereum/contracts/verifier/Verifier.sol

Commit ID: f783f571e16a1b1adddb13db45db741f83b94812

1.4 TEST APPROACH & METHODOLOGY

Halborn performed a combination of manual and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of this assessment. While manual testing is recommended to uncover flaws in logic, process, and implementation; automated testing techniques help enhance coverage of the bridge code and can quickly identify items that do not follow security best practices. The following phases and associated tools were used throughout the term of the assessment:

- Research into architecture and purpose.
- Smart contract manual code review and walkthrough.
- Graphing out functionality and contract logic/connectivity/functions. (solgraph)
- Manual assessment of use and safety for the critical Solidity variables and functions in scope to identify any arithmetic related vulnerability classes.
- Manual testing by custom scripts.
- Scanning of solidity files for vulnerabilities, security hotspots or bugs. (MythX)
- Static Analysis of security for scoped contract, and imported functions. (Slither)
- Testnet deployment. (Foundry)

2. RISK METHODOLOGY

Every vulnerability and issue observed by Halborn is ranked based on **two sets** of **Metrics** and a **Severity Coefficient**. This system is inspired by the industry standard Common Vulnerability Scoring System.

The two Metric sets are: Exploitability and Impact. Exploitability captures the ease and technical means by which vulnerabilities can be exploited and Impact describes the consequences of a successful exploit.

The **Severity Coefficients** is designed to further refine the accuracy of the ranking with two factors: **Reversibility** and **Scope**. These capture the impact of the vulnerability on the environment as well as the number of users and smart contracts affected.

The final score is a value between 0-10 rounded up to 1 decimal place and 10 corresponding to the highest security risk. This provides an objective and accurate rating of the severity of security vulnerabilities in smart contracts.

The system is designed to assist in identifying and prioritizing vulnerabilities based on their level of risk to address the most critical issues in a timely manner.

2.1 EXPLOITABILITY

Attack Origin (AO):

Captures whether the attack requires compromising a specific account.

Attack Cost (AC):

Captures the cost of exploiting the vulnerability incurred by the attacker relative to sending a single transaction on the relevant blockchain. Includes but is not limited to financial and computational cost.

Attack Complexity (AX):

Describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. Includes but is not limited to macro situation, available third-party liquidity and regulatory challenges.

Metrics:

Exploitability Metric (m_E)	Metric Value	Numerical Value
Attack Origin (AO)	Origin (AO) Arbitrary (AO:A) 1	1
Attack Origin (AU)	Specific (AO:S)	0.2
	Low (AC:L)	1
Attack Cost (AC)	Medium (AC:M)	0.67
	High (AC:H)	0.33
	Low (AX:L)	1
Attack Complexity (AX)	Medium (AX:M)	0.67
	High (AX:H)	0.33

Exploitability ${\it E}$ is calculated using the following formula:

$$E = \prod m_e$$

2.2 IMPACT

Confidentiality (C):

Measures the impact to the confidentiality of the information resources managed by the contract due to a successfully exploited vulnerability. Confidentiality refers to limiting access to authorized users only.

Integrity (I):

Measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of data stored and/or processed on-chain. Integrity impact directly affecting Deposit or Yield records is excluded.

Availability (A):

Measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. This metric refers to smart contract features and functionality, not state. Availability impact directly affecting Deposit or Yield is excluded.

Deposit (D):

Measures the impact to the deposits made to the contract by either users or owners.

Yield (Y):

Measures the impact to the yield generated by the contract for either users or owners.

Metrics:

Impact Metric (m_I)	Metric Value	Numerical Value
	None (I:N)	0
	Low (I:L)	0.25
Confidentiality (C)	Medium (I:M)	0.5
	High (I:H)	0.75
	Critical (I:C)	1
	None (I:N)	0
	Low (I:L)	0.25
Integrity (I)	Medium (I:M)	0.5
	High (I:H)	0.75
	Critical (I:C)	1
	None (A:N)	0
	Low (A:L)	0.25
Availability (A)	Medium (A:M)	0.5
	High (A:H)	0.75
	Critical	1
	None (D:N)	0
	Low (D:L)	0.25
Deposit (D)	Medium (D:M)	0.5
	High (D:H)	0.75
	Critical (D:C)	1
	None (Y:N)	0
	Low (Y:L)	0.25
Yield (Y)	Medium: (Y:M)	0.5
	High: (Y:H)	0.75
	Critical (Y:H)	1

Impact ${\it I}$ is calculated using the following formula:

$$I = max(m_I) + \frac{\sum m_I - max(m_I)}{4}$$

2.3 SEVERITY COEFFICIENT

Reversibility (R):

Describes the share of the exploited vulnerability effects that can be reversed. For upgradeable contracts, assume the contract private key is available.

Scope (S):

Captures whether a vulnerability in one vulnerable contract impacts resources in other contracts.

Coefficient (C)	Coefficient Value	Numerical Value
	None (R:N)	1
Reversibility (r)	Partial (R:P)	0.5
	Full (R:F)	0.25
Scope (a)	Changed (S:C)	1.25
Scope (s)	Unchanged (S:U)	1

Severity Coefficient C is obtained by the following product:

C = rs

The Vulnerability Severity Score ${\cal S}$ is obtained by:

$$S = min(10, EIC * 10)$$

The score is rounded up to 1 decimal places.

Severity	Score Value Range
Critical	9 - 10
High	7 - 8.9
Medium	4.5 - 6.9
Low	2 - 4.4
Informational	0 - 1.9

3. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	0	0	0	0

MANUAL TESTING

The main goal of the manual testing performed during this assessment was to test that the verifier is properly working to verify the zk proofs generated by the zkSync Era circuits, focusing on the following points/scenarios:

Test	Result
Check that using any valid proof, the verifier is able to properly	Pass
verify it and returns a true as a result	

(331481874871893334779187146986787444682614872732485561218923856957512686279, 124944317616188675127922198635625877455862686315986262777787732246451848859831315512185
14176619311997591532379426617975541851051754970955561673323057200623068374991, 942805240748-2545269453868343360556822214935716715779152167973895137167172 - [150] FECTOMPILE:resads(141764393189759153237942661797554185106173469696556167322305720066374991, 9428052407484754526945335634334052568222149357167157791521670738955137167172, 42542344970625915306574074847545554948347554947594575463951675467895789547897897897897897897897897897897897897897
- 816227862599707273786208675214437697885738078857380788511369572614899229775384829944, 1457338399972746585870622697924569938225862962567798524899387259
- 19371067795738147754269709708384173822106083881343915638425211941727574348135, 10096493883754872366665644510767983748468936775527044382272227309697811734964 [156] ### [156] #
□ - 1707/99881117/20728898542/04145852349/15147122146767198175247679485595997452, 410749579977188809779546641166515183137613856422254819228394795955919595952 □ 60899 PRECOUPELT: PRECOUNT (18858650806246839774929122363164751517559789155957993583915469579842, \$8097854769942441086515185913478593131785582112554555856786952 □ 60899 PRECOUPELT: PRECOUNT (1885865080644839774929122361364751517559789155979835931648) □ 70897448548211546827 □ 80897448548211
(staticall)
41794106\$7977710838979764511465515831373436954072544132343949798549194995522] [tatrical]] - a62388656419927981794092179499217938587986642209264927944127794452177956701974, 9888939619620942979375619469276392217805637282778965136956444212377444367939 - (60689) PRECOMPLIE::romul(220110863220837365555515124562044695579022033411133569115672278118482717978064, 1657565142353442355582927467244427789777585246531756531238820479997563983912, 79149796586549737522
[staticis]]
88893969196294297564846627639227789656667827278985148666444273327744496293 [istaticsall]
, 1755285798807454391802777385255880140644752831474494478389799014859358429277] [staticall] — 114754285558611802179588041880974518792179589921832294478165835, 181485894597459907286995082486552527215599796864975641879289984855184376666 — (54899 → (54899
- 46877375141807535288552404759266857909628194475911799849440777964159921796, 18110701902805824572713389141994565554478652755697913246079658872790801865 - [156] 187007011127760301(114974385588111021795838041889987475127317763897459153228447794165873874941465853, 1814859745974570872859765824685752773155987968649756418772897984685114376668, 468973951114675352863377864154978344844853344746362721538725856998978952334681477389771576470718] [istricall]
- 4771177406588455946130573404177395578040298852859885510406724514580866612337, 23948540229832921821201643001661855589061169526563774137797692754807339451 [6080] PRECOMPILE::compil(169549562437638572883231831250280961591394559954737843849411013513941834068, 7718063721694453053780323511979817841150752723427547762798662633617841278057, 411868069739115455705 [staticsall]
L + 201449661679228313071141035099042953713475374000591874979767000950407267749, 12747242372599213695720625707509996572584449611334670600412222536622414945252
- 5106972724663865134867887422957330748622778462789827858687878982785868787898278582789827898278982789827898278
L = 1663818628379659818533844290978946289789451878786619199421396857483855191188875, 7566411896177291189848718923274985411879794866815595587115431372985948398398 [1583]
- 786/270837802578046794224598085719422459808574742978932653947749934688471695827124317897288383938, 172218547659225398845529455266598497649558592859599585641865929839 - [6980] PRICOMPILE::ecual(63148612579893256394774993468847165862712865985686577674944269715832202429, 127242897097841174372897289477832883781556248942458194581945819486226, 18475452167710639295
123192802655815701349758579983826655153138017889448075519486552269632414386, 96534864965525749651626719680226859557316152697579179381816395655116685259 - [156] FECTOMPILE: reads(112318802655815781248758579828266251531380178891448075519480552269622414386, 965348649655257496516257196869226856517316152697579179381816395635116685259 - [156] FECTOMPILE: reads(112318802655815781248758579828266263154313801788914480755194480552269622414386, 965348649655257496516257196869226656517316152697579179381816396535116685259, 1495495862427638592885 - [156] FECTOMPILE: reads(1123188026558157812487585798832663515313801788914480755194480552269622414386, 965348649655257496516257196869226656517316152697579179381816396535116685259, 1495495862427638592885, 1495495862427638592865, 1495495862427638592865, 1495495862427638592865, 1495495862427638592865, 1495495862427638592865, 1495495862427638592865, 1495495862427638592865, 1495495862427638592865, 14954958624276385928665, 14954958624276385928665, 14954958624276385928665, 149549586242763859665, 1495495862427638596, 1495495862427638596, 1495495862427638596, 1495495862427638596, 1495495862427638596, 1495495862427638596, 1495495862427638596, 1495495862427638696, 14954958624276386, 1495495862427666666, 1495496666666, 1495496666666, 1495496666666, 1495496666666, 1495496666666, 1495496666666, 149549666666, 149
☐ \$\\ \tag{\$\\}\$\$ \$\\ \\$\\\$
(statisciall)
722154-7592725988-45237-9405246594-9464659777546955464623997785464585279687] [tatical] - - - - - - - - - -
3419581559011287979663872644564735647396464901896477946838947718688797216569779) [tatical] - 11558699816588171218575644898359613744444938981599521793135427769689773495459129, 35779882127459969537231561481322149474811719917622146241368592469723862121 - [136989] PRECOMP ILE: 30059912790159779415977941979966337383899744641864864564546895728976758999685316212897779858531691356914592739555866329971354499188151555996488178887, 1155973283299
1885624, 1885784699992395713594457876223239481378756359578518886998519993285655852781, 488236787586343368133229349314539563316851327593491286185741876214128993531, 84956599231234314176849732474892774384181995872
- (B) console::log(true) [staticcall]
$-\epsilon \alpha$

Test		
Check that verifier reverts with proof is invalid if a maliciously	Pass	
forged serialized proof is sent		

Test	Result
Check that verifier reverts with proof is invalid if less than 44	Pass
words for serialized proof is sent	

Test	Result
Check that verifier reverts with proof is invalid if less than 4	Pass
words for recursive aggregation input is sent	

[FAIL. Resion: los@Froof: proof is invalid) test_33x3() (gas: 132883)
Traces:
[C444990] Resistance() [
[C444990] Resistance() [
[C444990] Resistance() [
[C444990] Resistance() [
[C44990] Resistance

Test	Result
Check that verifier returns a true for a public input with dirty	Pass
bits over Fr mask	

(statio		o) PRECOMPILE::ecmul(13314818748718933347791974698070744466826149727324656612189283589578126862790, 1349414376161896751279221906335628979455862866918586262779787732244649184835, 54438898013155121895
[Statio	_	** 44174/191189795/19127974/24/19755-485186175449996564/79322857286472882974991. 9472852497442455249742557294254978554478757915124097389851747177 **TENTIFY OF THE TOTAL STREET AND ADMINISTRATION OF THE TOTAL STREET ADMINISTRATION OF THE TOTAL STREET AND ADMINISTRATION OF THE TOTAL STREET
11996096	9715655:	49814780816786577566863689914271293017405504676884392297646) [taticall] - 980179509168077777791948797141203047977879787917879787917979779797979797979
[statio	_ [686 CCall]	9] PRECOMP-16:1:exam/(5552003306751162852086397237551787264885777962751791299169104491249527115, 110499275148135877164916475263757796928097773646092490449980976745688374, 162543798809580413159
	-	** 1971/04/79873814/7784/2097997662304/7981/04/5097997662304/7981/7981/04/509799762304/7981/7981/7981/7981/7981/7981/7981/7981
14573383	_	6685700202692746670882226027657789747948868507715823027387259) [ctaticeal] - 4707879888117272727888562744145823242151471321476777891727677470778507974159
(static	call)	0] PRECOMPILE: acusul (188884880244538774932913226316047151775597839150259932835231583839316669872843, 35093864076904344108465916589319488801317852543126346515928097882222346518928097882222345483, 2058944054482125460292
	- (15	- 4511317857447482584433994784556446751868078777411744597924459965769775865, 1191745781521779782851417205556135218270644178535613521827064541720553927942758463094044625417, 1767896851117267258855 PECOPUPLE: 15760464(\$8511243556744442584459974974565667587974696965777477677686), 2191745781612779782864141795859636441795585963044617257587694641795876787648417978769681117267258855 PECOPUPLE: 1576046(\$8511243567544425854699749745656675774479770486967774479676969), 21917457696974969699999999999999999999999999
12941869		88907966611665158317713087606275419723457967965549786552916395522] [raticoll] - 2-21889545197998174097523978696527297839789652729789679797979797979797979797979797979797
(static	call]	0) PRECOMPILE::comul(226110836/22038730555551514286204460359032083101113150101569217311040171979004, 165756514235314335558292407242414973807756524063176633128062049893765983912, 791499058868497375234 - 287074041386759274698390408679666510683460608310469740220624228560422404679, 9018823855780213367405135187734467489611554651074667305571347702735130740570
8802040	- (15)	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	_	* 1189/350440613657/445256452118320667/382884476856377946485177961179675142277276, 1785/087988074459127778852588681436804725811474097478332799014069388-89277 **PROUND
176520	37988074	149918279788515588814864927823147449747838293890148967854829279] [Iristicall] - 1199478695850811091779688940189897831792317948789184252847914668585, 18148589465945978972869786824865525527315570877860649775641877287084855144376668
	- [68	0] PRECUPELE: recumu(d, 2, 518899418587145157153947711855652637233386688188657348978465711463879502) [statice31]) - 40897358114107457528585524679766868210474758115978497446777146191103208852657312858114791652568476652563957912264079608588737808681855 - 40897358114107457528585524679760858873780868184559944647798615978911032088952673712858114791652568476652563957912264079608588737808681855
37780415	5698334] PECCOPILE::casd(11943985658311017704580418899947812931704399336322044798163878974941466835, 1814858946594590072868965248658258527315590970606497564187928900485184276660, 460973951104675852885
	_ [681	47711774065884597441897349687340417739857894627985238579865184089724514608860412322, 2379454042798252272127161446881645185585974119765652774137707692754807239451
staticc	, L	© 20144966167928813071141035099642953713475374000591574979767099005407267749, 1274724227258921360572052570/5009806572584449611334670600412222536622414945252 → ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
23948546	92298326	21921200430806420855589041109530565277462778040927840973394531 [[128][128]] [[128][128]] [[128][128][128][128][128][128][128][128
staticc	- [686	0] PSECUMPILE::ecum)(631486127709832563947749934168947108562712069035685677674944269715893202439, 1772628070070414743755522094977961828947438838778155624944255196551934804225196518348042251965518348042251965183480424519655183480424519655183480424519655183480424519655183480424519655183480424519655183480424519655183480424519651804040404040404040404040404040404040404
	- [156	* 16638166/28779659946583394427996759442590789461579706461919942139057448355191188875, 7566451189641779791849271897274955111979794663155955587115421372986948383939 PRECOURLEIT-E-MONITORING TO THE PROPERTY OF THE PROPERTY
23487147		786568276852276954755685598781565583475518972877886574897827944) [staticall] - 7869628572985988059475259886919472568598279456485582747563485586294928978598949498978959899999999999999999999
(statio	ccall]	8) POLICION 1.5: x = x = x (6214611576972256594774972416814710566371746993668657767404426971685204427, 1272238768744174375557289467799818294747288887741502469446314634684674674674
	- (158	- 1123/3800/25581570134755579938274655153128173891440755149465522674623141346, 94534044945555749451457719468224685557715157469525779173818145746757177381814695557 100000001161:1000001(1123193802455615781349758579383264631531388178974489755174865234748241386, 9453464945515717946822364565517316152467579179381816395435114685559, 1695495862437638592832
		E886623112371672411091727431724917947962368174738997/F4074581734896795974164811 E88662311237167832919151646858982378794812128685268615497285794295979459594, 184686613188288259256127855946991838473938417383368319687856678257384558564 6) PRECOMPILE::ccuul(22577208226254499394144638547438993974277412892272577452554483227089253884, 9891218761914748522381969127861446391756173452977615861129552313284917562538, 1348513438679857386667
(static	call	## 58241342484238645873872342497397582386552246184423864782727238297488848582399924773774425589789718315138885736727489572978582988888658397
22185476	- (150 65932531] PRCOWPILE::codd(6824184294823065857857240473779592865592244642256767327230197880853465918, 644963482399734773796424548927871531513803512602877974055229035020556055635552436422567673272301978808591943
	_ (68i	- 1987/03/1887/541199766043792009/1601864556446905232994625997686597686216121007275, 19181/15584477798586216912561452739258566210921154499188151559994160176007
[statio		- 7057467787856428899027391761880294467678371148908644421997881736694664951456, 1822786386586482878658925182488214995438258437857647245267286549738976824956
195815	53011239] PECOPILE::ecado(PEC/40787864288900273917488024-04678271489084442197788173649051464, 10827563645084387405075188248921497648323643754452472865490789789378934956, 5086632142347158783293
205.00	- [113	- 11550/0456581721857564008596718740040700082159221721854276460877249556120, 38777892127459046757215541813221494714851171901762214654113656524607230651213 0498] PRECUMPILE:::epuning(1987708158775411999466327083094146618646554446865236799625575966852161290737315419715684477795858463289125644579721884519585763 04999230971357445707722323946137075659575815886599651999235565585781. 408923678758634236813223094081145767824789724789724789724788145199857763
20034,	1085/84	
- 1		ole::log(true) [staticcall]

Test	Result
Check that the verifier returns a true having elliptic curve points	Pass
over modulo	

Admon	90013155121095
+ 11764/3911897951532797426417875541581561754699955541273223867396927999, 92482549754784729542362492362234982749872178521678788788137167157 - [159] PROCEEDIL: 11764-118785418751532279426417875415186175449965556147782308673968230857399(7), 924882549742495425629423582343823482562562221498751671797815116778788985137167177, 42543244	07047501520595
19969997156551498814259816286579568686368991422122938174835845768433229546) (staticcall)	
	98803580413159
\[\frac{150}{250} \] PECONFILE: scadd(1971047795738147754267907692804738216068382104075521041727574248185, 1809649388275487236666544510767982748489936775252904882272227309607811724964, 31022291 \] \[\frac{150}{250} \] PECONFILE: scadd(197210477957381477542707067693847382160683882134931563845221041727574248185, 1809649388275487236666544510767982748489936775252904882272227309607811724964, 31022291 \] \[\frac{150}{250} \] PECONFILE: scadd(1972104779573814775426790767683847382160683882134931563845221041727574248185, 1809649388275487236666544510767982748489936775252904882272227309607811724964, 31022291 \] \[\frac{150}{250} \] PECONFILE: scadd(1972104779573814774426790767683847382160688882134931563845221041727574248185, 1809649388275487236666644510767982748489936775252904882272227309607811724964, 31022291 \] \[\frac{150}{250} \] PECONFILE: scadd(1972104779573814774426790767683847388475847687678578767878787878787878787878787878	86250970727378
	54487175460707

- (150) PRECOMPILE::ecadd(4351126137657442482584633994784536646781086078777411764597924489065760775068, 2149174878182179748820641412033561362183206345417295539629427598486940646617, 170789001	81117267258035
1294:1807/971718889027084664110455153313741885340275481732439959529 traticall	
	58868497375234
□ 2899749413867592749989069697964695186833869949226632285689322685479, 051882385578821338748513815734467499611554681974467385571347767953139749579 → (15) PRECUPPELL: tracead/(2899744936759744957496946974696451069432686481969462769467496155574467469515571447767951397449745155474797451347749735139749579 → (15) PRECUPPELL: tracead/(2899744936759749669746646796469469746974697469746974	41902980179409
8883901/42/0942975619466027403217896064793278805140596444212327744840393) [stational] 1 1839354646136574748254682193286973832967338295319931179937514227276, 17952087988974649188279738525588214364925231474499447833939901144697369439297	
[456] DEC.	04061365747482
- [4000] PRECOMPILE: secus[1, 2, 518890418857145157,15979711855852/397123380460818865734897749573111668795209] [statice31] - 4.6697395114867552868552469796360857909636091447797128559927105, 181120139288526577312856149746652586395791326649768588973708001365 - 4.669739511486755286855246979636085799636857897408578149746652586395791326649768588973708001365 - 4.669739511486755285852649763608578785897497897185978971859789789789789789789789789789789789789789	
- (150) PRCOMPIL::recas(d14954955593110217965894618990478212931796899318922044798163873874941468635, 18149589465945909728639568248655255273155987986044975641879289084055104376666, 460973919778784485838947639267212853275685969092032336808197389715206478] [tatchical]	51410675352085
	93391154557899
Tatics - 2014496612792383138711418359994275271347557400859187497976708790085467267749, 127472423725892126957206257875099865728444961133467060041222753662241494552	
[150] DECUMENTAL: ecost(2014/0644/7023831307144/08509744/7057154/70574) [171774/207589213697240277599865725844061133467060841222536622414945252, 4771177.	40658845594613
- \$184687274462465124875274575307462727642767573788807766728817468766, \$127867748764674976527684272646751488767786726787878878878788788788788788788788788788	
staticeall)	9088908\A09018
□ ← 16688180/28379609+885384-429697564020974451579766411994-1239457443855191488273, 74664411964777201139284718923474965411979446648155076557115431372696948398399, 519659222- □ 1569 □ PRECOMPILE: teaded 166381820620274569748538384479967564027964158759640196413796576493551183887, 75664411964777201197846119677940668151507964011979140197914019791197911979119791197	46636651349878
24821/7482464249365482749554275865598131655374756199297986574979829941 [statiocal] - 7-86792887980798989899898989898989989899899899899899989999	
[484] [486127:0982756] [486127:09827563947749724168247108562712069035085677674944269715032202429, 12726280709704147437535920949799818209474928838776155024094245019658103406226, 1847545; [486126767676767676767676767676767676767676	21677106392937
- 11231/3802455615701347857893824565157013837857893224455132018075194655226703241480, 965334046552374951425724648522679513724685226965157013487852655157013487857989322445513201807894552701446552596794554257104685259746542571046852695157013487852651570134878579893224455132018078794526797104685270146572679710468527014665726971046852701466572697104687104671046710467104671046710467104671046	24274205020022
1866/37/1694450857/882355119798178411867782924754792986921947986921947198797 [:satire.all]	240/0000120002
- [6000] PRECOMPILE::ocmul(2257920826825449939414463854743099397427742128922725774525544832270890253504, 90912187019147485323319691270014746391756173432977615061129552313204917562530, 134351343	30079057386667

- (150) PRCUMPUL: read(60/414/28423045873572/44/3797959265522/46/42256/76/327/30/19/88063455910, 644963482399347737944245489/97/153151380351260207797405522903502058640565074, 7069208371	00259800591943
☐ 19877981587754119996663270809041669286656468805738299762585996883162120807275, 19182/1559447779838631691356014592739525863299721154499138151555994489176909 ☐ (49699) PECCOUPT II: : : : : : : : : : : : : : : : : :	43997995738666
[\$\frac[0.21]] - 7057-4677879564-2880992739176189274-676783711489084-64-219978517366946649551456, 189275430658843970658925138248521497543825485714975438254497547345267286549738975834956	
(150)	42347158783293
- [1130ee] PRECOMPILE::ecpairing(197783188778411979663378308904160813605444691235979425597806853162120877375, 19181715584177798586831091360415327935286422097211644971881551559704801740977, 19181715891477798586831091360415372935286422097211644971881515559704801740977, 19181715891477798586831091360415372935286422097211644971881515559704801740977, 19181715891477978586831091360497879, 191817158914779785868310913604978789, 19181715891479789, 19181715891479789, 19181715891479789, 19181715891479789, 19181715891479789, 19181715891479789, 19181715891479789, 19181715891479789, 19181715891479789, 19181715891479789, 191817158914799147918914799147991479914799147991	
□ ← 1 □ ← true	
(0) onsole::log(true) (staticoall)	
L+0 "	

Test	Result
Check that the verifier returns a true, having Fr over modulo	Pass

├ (6000) PRECOMPILE::comul(13314818748718933347791974690070744466826148727324055612103203589578126862790, 13494143176161086751279221906335628979455862060313506262779787732264649194035, 5443889001	3155121095
[staticas11]	
- [150] PRECOMPILE::ecadd(1417661931189759153237942661707554185105175469965561673323057200623068374991, 9428052407484254526945335634336052568222149357167157791521670738985137167172, 4254236497062	2591530585
197690971565514798142857916208636389714221279801748564617684332279546) [raticall] - 818227986159977777378620857414390873873577048519159727978459997277786598370972778659870972778697878784139678797878784899974774659870972797878978784139678797878499972778459879787841989797778459979778459870978778698979787845987978784598979787845989797878459897978784598979787845989797878459897978784598979787845989797878459878789897978784598798979787845989797878459897978784598979787845989797878459897978784598979787845989797878459897978784598997787845989797878459897978784598979787845989977878459899797878459899787845989978784598997789899778999787845989977899979789997978999797878459899797889997789997787845989977899977899979778459899778999777845989977784598999777845989997778459899977784599979797845999777845999777845999777845999777845999777845999777845999777845999777845999777845999777845999777845999777845999777845999777845999777845999777845997977899977784599977784599977784599977784599977789997778999777845997977899977789997778999777845999777899977789997778999777899977978999777899977789997778999777899977789997778999777899977789997778999977789997778999777899977789997778999777899977789997778999777899777899977789997778999777899977789999777899977789997778999977789997778997779997799977999779997799997778999977789999777899997778999977789999777899997779999779999977999999	
- [6000] PRECOMPILE::ecmul(5558200330575116285280683972373527873648857779562751792429916910431240322115, 11049922514813389721684916475263757296982809777360609249044998037079645088324, 162543798803	3580413159
{rainiciall}	
= [150] PRECOMPILE::ecadd(19371067795738147754269790760330473832106083881343915638425221941727574348135, 1009649388375487236665644510707983748408936775252904382272227309697811734964, 810222986256	0970727378
4573383997727-668587802026/279-656903802260279-656903802260279-655755558280278375595 [statical]] \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	
- [6800] PRECOMPILE:::comul(1086866802645307749229132263168471517755976391502597922035221583803916669872843, 8589738564078990434418946591658923194088091317852843126246515923607803222345403, 205894405448.	2125469292

- [150] PRECOMPILE::ecadd(4251126137657442482584633994784536646781086078777411764597924489065760775068, 21491748781821797488206414120335613621832063454172955396294275984869404063617, 1707890081117	7267258035
294 6571108889798664116451518312761385364225481923639672855219164395522] [staticall]	
□ - 36.2308564.19273817940621738258778066.2382765412779445217796761994, 988833691962692293756194460.2783728271886527282738951629564431232774046633 - (6808) PMECUMPILE::ccmul(2261188362203873855551542862044603599329331811131501815692278118481719279894, 1657565142353143355582924497424142973897758524063175633128802449973763983912, 791499658661 ***Total Computer Statistical Computer St	8497375234

- (150) PRECOMPILE::coadd(2899740413867592746988906006796669510684348060831069940220634228560432604679, 9018823855788213367405135187734467489611554681074667305571347702935130749570, 36230085641902	2980179409
882950919420947293756194466427630212788663778878696512695664432123237404465939) [ctatice:il]	
- [150] PRECOMPILE::ccadd(21785981531948761494559609919037245937097418924234616328608264160875841695031, 12017340029476537792548200911119210915442407378081009302568808208368778719941, 118393504061	1365747482
1755203798807454391823797385255880114360475238147449944733297309014067556432797) [ratical]	
- [6000] PRECOMPILE::ccmul(1, 2, 5188996185871545157153907711855052637123330660818865734897946952111668795202) [staticcall]	
□ 4.6697.73951.4186773852285852460-7698466857899663194.747581.12799494.44777904.1599431794.1581.8112/241.36285632657372.32881.4199456.22586478952.3258.37971.22646794698387373969041855 1.559.97820491.512.15.256.0041(11.9478.34855684)1120974.97841792371796399213220447981.53873874944469855.118.4186934459549979724899632945555552731559974966449756441879239904055104276669. 4469773951.418974567855678418772399040551042784187923990405510427846985.118.41869344595499797248897623955555557257559974066449756441879239904055104276669. 4469773951.418974567855678418772399040551042784699. 4469773951.418974567855784187723990405510427846985.1188745874569874646985.11887458974869974646985.11887458974869974869897486999748699748699974869999748699974869997489999748699974869997489999999999	0/75050005
77864156983344864853384768326271253822565898992832336881877385771526286718) [staticsall]	00/0002000
□ « 47711774e558845594412867346417795878844299852859886194e9774614588866212322, 23948546227982320182120144380166185558794114595265637743277976927543697339451	**E*EE7000
tericcall)	.154557677
□ 201449-661679223813897114198589794-279537124755740895915749775708979805497267749,7274724237258921369572865787509785572884449611324670868412222536622414945552 □ 1599 PRECOUNDEL Inc. Located/2014/1946/679223813917111918809749-259571247557408069197247747242372589213697926575787507869986575824494613324670800412222536622414945552 □ 1599 PRECOUNDEL Inc. Located/2014/1946/679223813917111918809749-2595712475574080619762477424237258921369757265757869986575884494613324670800412225366622414945552 □ 1599 PRECOUNDEL INC. Located/2014/1946/679223813917111918809749-2595712475574080619762477424237258921369726785786985786986912225366622414945552 □ 1599 PRECOUNDEL INC. Located/2014/1946/97283139187497474243778695136978698677869867986987869869878698989898	00/550/442
39485482298320218212016438016618555890411695265637741377076092754807339451) [staticcoll]	0040074013
□ 5166892224653665134687887432757326748622784627698751379682077667298821748656669, 512248714782365629736527682276825347651907269708674573827964 □ 646991 PERCOUNDIT: :: newsul (6314846127670827584471698624718686271946475882)2019209708179414174378537857904979981839047427368878737851856924697487881824662764 □ 646991 PERCOUNDIT: :: newsul (63148461276086275864276982716986276864669, 512248714788627646978568678698818246576498678678678648698678698698686868686986986986986986986986986	4407045440
10889 PRELUMPILE: COMUILOS 1480125/89832503947/49394105884/18586/1280988505/0/4949498/1510832/8444428/1510832/844443/55978949/9413/43/55978949/9482844/43/858789499/9482844/43/85878949/9482849/8444/848887/8150824944/43/858789/8444/848887/8150824944/43/85878949/9482844/43/85878949/9482844/43/85878949/9482849/948849	008/905018
□ 6.645816028279659046533844270e078046200704515707066(1919042129057448355181188875, 7566411006417727118794871897237495841109797406631559558711543137206504839239398	
- 1300 HELLOWFILE::COBOLIDOSSIBLES/NOOPH-8553844/980/9004/9005/1704/13705/0483951011888/5, /3004118001//7/1187048/187/5/47804118/774800810379005/1104313/800948378378, 518087/2/240081	00513488/8
	740400007
Today MeLUMM LE::ecmul(bs1480120/8785205947/4978410884/189582/12807858988067/0/4744208/10852281427, 12/2028/108/88147/43/550728747/97852874/4328858/8105824874/208588/8105824874/20858/810584874/20858/810584874/20858/810584874/20858/810584874/20858/810584884/20858/81058488/81058488/81058488/81058488/8105848/8105888/8105888/8105888/8105888/81058888/81058888/810588888/810588888/8105888/8105888/8105888/81058888/8105888/810588888/81058888/8	180392937
□ 1123/9882/0568157913/487688759983826465153138817389440975517406572349632444300, 955340440955527496516/5719406823469555173405246759179831814639665811404695294	1005000000
1004 1005 1005	0385928832
☐ 5-5464632142347158783293188488589827797941813408536395140477857697959754455954, 1844684613188289359756127855599409188847898417383340319488978546789257984558584	005700///7
- [4080] PRECOMPILE::ecual(225792828254499394144385474380939742774212892272577452554483227889253504, 900121870191474852231901778014463917661724329776150611129552313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 134351343007761504112952313204917562520, 13435134300776150411295231304917562520, 13435134300776150411295231304917562520, 13435134300776150411295231304917562520, 13435134300776150411295231304917562520, 13435134300776150411295231304917562520, 13435134300776150411295231304917562520, 13435134300776150411295231304917562520, 1343513430077615041129523130400776150411295231304007761504112952313040077615041129523130400776150411295231304007761504100761041129523130400776150411295231304007761504112952313040077615041129523130400776150411295231304007761504112952313040077615041129523130400776150411295231304007761504112952313040077615041129523130400776150411295231304007761504112952313040077615041129523130400776150411295231304007761504112952313040077615041129523130400776150411295231304007761040000776104000776104000077610400007761040000776104000077610000000000	/80/35000/
► 5024134284823065587357324947397959286525224616442256767327230197680063465910, 6449634823993477379642454892987153151380351260207797405522903502058605653074	0000504045
[150] PRCOMPILE: reaso(S024144284238055873572249473797952355522446442256767232723819785866346518, 6449634239924773796424648929871531513803512402877974065522983602658065652074, 706920837802552248478920871531513803512402877974065522983602658065652074, 706920837802552248478920871531513803512402877974065522983602658065652074, 706920837802552248478920871531513803512402877974065522983602658065652074, 706920837802552494789208781531513803512402877974065522983602658065652074, 706920837802578247879740678154087892087758047892087780478789208080808080892087892087892087892087892087892087892087892087890808089208789080808080808920878908	0000591943
- (680) PRECOMPILE::ecmul(1618384989994043818949359838767911976672882599560690820245389499286765021563, 320109355679696266759850531176732990872308033146738631772984017549983765305, 134351343806751676187618761876187618761876187618761876	7985738666
☐ ☐ ~ 7057469787056428809027391761802944676703711489086464219978817366946649551456, 10327563665084387065092518824882149954382354375376473452672865490738975834956	
- 156 PRCCOMPILE: scass(196746797816547288098279977518807946767897114998846421979817368946649551456, 1832756365688438786589725188248821499543823854375376473452672865498738975834966, 5836632142341958515531239297663326436473565039794673637971854734565897918547346379185473457854734557818785487854878548785487854878548785	158783293
	.7
66.41 [15:000] PECOUPIL:::copxi:inu(19377031557754.1199966037953094).160118-66544468052379975597668571012007375, 191817155944777795586231091356445527397578662370921154-991883151559944801790075059668571012007375, 1918171559447777958862310913564455273975786480791075470727478077778787878787878787878787878787878	7732032986 8190587263
L+1	
- true - (8) consoler:log(true) [staticcall]	
└ ← ()	
— ← 0	

Test	Result
Check that verifier reverts with proof is invalid if more than 1	Pass
public inputs is sent	

```
[Fill Teason: laudFroof: Proof is invalid) test_bx() (gas: 152154)

Traces: 
[4.449728] Pointset_bx() 
[4.449728] Pointset
```

Test	Result
Check that verifier reverts with proof is invalid if empty public	Pass
inputs is sent	

Test	Result
Check that verifier reverts with proof is invalid if more than 44	Pass
words for serialized proof is sent	

```
[448723] Point:sextin()

[448723] Point:sextin()

[448723] Point:sextin()

[448723] Point:sextin()

[448723] Point:sextin()

[448723] Point:sextin()

[448724] Point:sextin()

[448725] Point:sextin()

[448726] Point:sextin
```

Test	Result
Check that verifier reverts with proof is invalid if empty	Pass
serialized proof is sent	

```
[FAIL, Reason: loadProof: Proof is invalid] test_TX() (gas: 28877)

Troces:

(64-09728) POI::string()

(74-09728) POI::str
```

Test	Result
Check that verifier reverts with proof is invalid if more than 4	Pass
words for recursive aggregation input is sent	

Test	Result
Check that verifier reverts with proof is invalid if empty recursive	Pass
aggregation input is sent	

Test	Result
Check that verifier reverts with proof is invalid if elliptic curve	Pass
point at infinity is sent within the serialized proof	

Test	Result
Check that the verifier reverts with invalid quotient evaluation if	Pass
an invalid public input is used	

Test	Result
Check that the verifier reverts with pairing failure if an invalid	Pass
recursive aggregative input is used	

□ - 4.41764/9211897591523797426641767554158168517846796556161732238572086278086374991, 9478085246748275452694538564323685568272149357167157791521679738985137167172
□ + \$182279842569797777378244695734443964738573876811365892674897229776738427944, 145733839797774666857802207974569889204974567895678567856785678567856785678567856785678
[staticus]] - 1937164779673814775426799768384738321968388134391563847521941727574248135, 100964938837548723666654451076798374846892677525290425272227309697811724964
□ ** 37078700881117377558036264416552344121847122144727198175247774825505876174124*, 1129441697079171888927596561165151831271.0855662254815122363970595591959591959195919591959195919591959
[*ratics31] - 4541261376574424825846399478453646781886878777411764597924489065768775868, 2149174878182179748829641412835613621822863454172955396294275984869484663617, 170789968111726725886 - [159] PRECOMPILE::cc.mbg(43511261376574244825846339947845366467818886978777411764597924489065768775968, 21491748781831179748829641412833561362183286345417295539629427598486948663617, 170789968111726725886
1294186979A7171888892768664114651513313773189586725849124262784519242627845192426784517945785179567919394, 98880379591042694292756184686277630221788653728758865428217377449486939 - 40210868564190298017449021738589704664280162623446734127746184517795679194994586849737522 - (6000) FRECOMPLET: comuni (22611083622838738555515142863844683599320331811315801569227811848171929094, 1657565142053142355829244129778977885248631756331288820498937639838912, 79149996586849737522
[484]cosil - 280974041386759274988984086796495146842480683184994022062422856442264479, 9018823857882132674051518772446748961155465129746729551207497629512074978996980679649514684248060851849940220624228564422684679, 9018823857882132674051518772446748961155465129749789295120749789789896086796695186842488068518699402206634228560422684679, 90188238578821326740513518772446748961155465129749789285128747782978512074978989608796695186842488068518699402206634228560422684679, 9018823857882132674951351877244674896115546512978787898789898989696796695186842488068518699402206634228560422684679, 9018823857882132674951351877244674896115546512978913477829512074978989898989794678989898997946789898989999999999
888956196209419737561446662748922170965627287289661369564431232744866999 [ratical] - 1189795846136574748255482133230597388289476823978346817899119973514227275, 17852037988074539109279735525580314264253831474499447832939907146927854952997 - [158] PRECOMPLE: raceast (21789995185144975586860671987745933997418924274616328668244160875814195983, 128173468244763779254828091111921691544247378881809305568808288368778719944, 11839350446136574748
1755282788874843918277978852888214269425831474499447538289914469788482797 [statical] - [4196430855801101795580401030876179179179898754522844798158878914917981588789459459459072889956242655155273155987996064975641879289004055104376660 - [4000] FRECOMPLET: count (1, 2, 5188994858715451571539877185085626712338060851886572489794695111468795492] [statical]
- 4.687773541467735214855244477966528524447786179844644777964159981745, 1811020130228682457271335814197465255847865225639579132664579665883737686818565
- 4771177496588455944129572494177379578944298552899886519409274514598866912322, 239485402298239218212916439816418555897941195125656774127767692754897237451 [6000] PRECOMPILE::cross1(16954958624376885920832318312562899615091394559954737843549411013513941834688, 771366372169445395370832351197981784115975272342754736298692633617841923057, 411068009339115455709 staticabili
□ □ 2014A661677228331287114183589964209571247574686959187479776789798687267767, 1274724237258921369572854575758998657258444961334678680412222536622414945252
- \$184882224653651348673874229573874682278462769875127862877607296317466469, \$12248714785365437495246549553885598181555347551897290786574592994
- 1663816-02037965904853284-279007546-0200796451707964511904121957486255101188375, 7856441196417729118984871897237498841187979406681559555871154313770956488298298 - [150] PRECOMPILE::cc:sdo:(1463818628379559484538342799675644289748451597096451199447139457148355181188375, 7566411964177291189848718923749854118799446681559555871154313772095848398398, 5186892224663665134887 2248714785636249785562798527269854725269859513155534776510972097085574857382994) [craticall]
- 706020837002598005919432095083949842809594733114937297501714313789728383938, 172218547659225398084532949520659849665392775536065586206239957856010859299080 [6408] PRECOMPLICT: excutl (651861257098255639477499341688171458627128678345085761749442087158321282429, 1772628978078411742755572894979981820947425883877815582489424599458183486726, 10475452167710639299 [atticizil]
1121093802655915791347585790838246351513801789944075513904555239042241986, 965346494552574965162571946622369855517316152407579179381816395635116695259 [156] 97654664763655714966523696525749651625719466523696555714051695269517316152407579179381816395635116695259 [156] 97654664763657164463652769612571946652369655574965162571946652369655712465236965571246523696577149667714967714967714
- 58364321423471587832931854885993278794181260853439516472857692957754455954, 184886431882808592541278559969971888478984173833693196878560789257384555594 [6080] PRODUPILET: eccuni(1, 2, 18485184980797973866737718857897188577971887838348478568725895923) [catacical] - 216482233633898796767365978662729244562117429072752844847379746778545297. 252244673845429718793846117564377884244818495757847187427771787
(150) PRECOMPILE::exadu(2104022336330268790673657648662479249436619114290175268414867399469785452029, 25524467836436914290354409947834611576643778842440181495757847187427771787, 78692083700259808591972212815592353780849249782145708590476689327776508658582082209975866018085790939 [taxical] - 204536565483973397455521547876780861406585926382182508418866975. 5588942728552360984392684995741923683477540774065764752712470823464778083956
- [6000] PRECOMPILE::ecuml(1, 2, 134351430079057386667372106851689710865797108677370687034067487668725395928) [staticcall] - 110402723633201589796673265543006247274476615141790477526444657379746778545202) 27234467364869708738461515766437788424401814975787847187427771787 - [1500] PECCOMPILE::ecuml(1, 2, 1343514300679067386467372406673788424460147067878467377887187427771787, 503663214234715878327 - [1500] PRECOMPILE::ecuml(1, 2, 1343514390679067386467372446619147906785452027) 272446786469978364415766437788424401814975787847187427771787, 503663214234715878327 - [1500] PRECOMPILE::ecuml(1, 2, 13435143906790673864673724066737846746619786747864786478697867867867878678786787
4195815558012392996336261156473562839964694459617916938184771698397921698979) [statical] - 1169585697345279863573975847756557984375721698379721698979) [statical] - 11695856973452798635739758477565573975856584275873858864275467278378587279857311271527588631616324977565579943097561572908977525 - (137986) PROVOW [115, 10000117] [126958548398793873585543214567986464497586457782331271575657329857784697978497774657747847774677478477748774877478737449778837956, 115597320270857846979784778657978477846774867746677478677486777486774786774786774786774786774786774786774786774786774867747867747867748677478677486774867748677486778677
06523_18570440999223871359445707622322374813707665596785188986996519992285665852781, 40823678758624326813922834931454355683168513275924012881807418762111200928511, 84956539231234314176049732474892752438418190587265
- finalpaing: pairing failure* - finalpairing: pairing failure*

AUTOMATED TESTING

5.1 STATIC ANALYSIS REPORT

Description:

Halborn used automated testing techniques to enhance the coverage of certain areas of the scoped contract. Among the tools used was Slither, a Solidity static analysis framework. After Halborn verified the contract in the repository and was able to compile it correctly into their ABI and binary formats, Slither was run on the verifier contract. This tool can statically verify mathematical relationships between Solidity variables to detect invalid or inconsistent usage of the contracts' APIs across the entire code-base.

Slither results:

ethereum/contracts/verifier/Verifier.sol

```
Reference: https://github.com/cys/striferr.cole3) allows old versions
Propas version*0.2.3 (src/verifier/Verifier.cole3) allows old versions
Propas version*0.2.3 (src/verifier/verifier.sole3) allows old versions
Sole-0.2.17 is not recommended for deployment
Reference: https://github.com/crysic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
       Mercanes: Notary/astubus.com/crysts/lither/wisi/Descetor-DocumentalineFinorrest-versions-of-moldsty
MPG/Descetor-Fire verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage (inc. verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage (inc. verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage (inc. verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage (inc. verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage (inc. verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage
Parameter Verifier.verify.ass_2 reverbitibless().point_verify.ass_2 reverbitiblessage).ln.verifier.verifier.verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage
Parameter Verifier.verify.ass_2 reverbitiblessage).ln.verify.ass_2 reverbitiblessage.ln.verifier.verifier.sols2300 is not in mixedCase
Parameter Verifier.verify.ass_2 reverbitiblessage.ln.verifier.verifier.verify.ass_2 reverbitiblessage.ln.verifier.verifier.verifier.sols2300 is not in mixedCase
Parameter Verifier.verify.ass_2 reverbitiblessage.ln.verifier.verifier.verifier.verifier.sols2300 is not in mixedCase
Parameter Verifier.verify.ass_2 reverbitiblessage.ln.verifier.verifier.verifier.verifier.sols2300 is not in mixedCase
Parameter Verifier.verify.ass_2 reverbitiblessage.ln.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.verifier.veri
```

• As a result of the tests carried out with the Slither tool, some results were obtained and reviewed by Halborn. Based on the results reviewed, the vulnerabilities were determined to be false positives.

5.2 AUTOMATED SECURITY SCAN

Description:

Halborn used automated security scanners to assist with detection of well-known security issues, and to identify low-hanging fruits on the targets for this engagement. Among the tools used was MythX, a security analysis service for Ethereum smart contracts. MythX performed a scan on the verifier contract and sent the compiled results to the analyzers to locate any vulnerabilities.

MythX results:



No major issues found by Mythx.

THANK YOU FOR CHOOSING

