HashEye

// SMART CONTRACT SECURITY AUDIT

EthStaker Deposit CLI

Security assessment by HashEye · prepared for EthStaker

HASHEYE AUDITED

PROJECT	EthStaker Deposit CLI
PERFORMED BY	HashEye Security Review Team - Sergey, Brian
RESEARCH	Sergey, Brian
CLIENT	EthStaker
CATEGORY	Blockchain
PUBLISHED	December 1, 2024
REPORT ID	research-ethstaker-deposit-cli-2024-12-01-z69oic

This report was produced by HashEye's security review team under the HashEye review process, combining source review, deployment-state checks, and senior manual verification. Full report detail is available at hasheye.io/audits/research-ethstaker-deposit-cli-2024-12-01-z69oic.

ULTI SecurityAssessment(SummaryReport) December27,2024 Preparedfor: 0xStef ULTI Preparedby:ElvisSkoždopolj

Abouthasheye Foundedin2012andheadquarteredinNewYork,hasheyeprovidestechnicalsecurity assessmentandadvisoryservicestosomeoftheworld'smosttargetedorganizations.We combinehigh-endsecurityresearchwithareal -worldattackermentalitytoreduceriskand fortifycode.With100+employeesaroundtheglobe,we'vehelpedsecurecriticalsoftware elementsthatsupportbillionsofendusers,includingKubernetesandtheLinuxkernel. Wemaintainanexhaustivelistofpublicationsathttps://github.com/hasheye-io/publications, withlinkstopapers,presentations,publicauditreports,andpodcastappearances. Inrecentyears,hasheyeconsultantshaveshowcasedcutting-edgeresearchthrough presentationsatCanSecWest,HCSS,Devcon,EmpireHacking,GrrCon,LangSec,NorthSec, theO'ReillySecurityConference,PyCon,REcon,SecurityBSides,andSummerCon. Wespecializeinsoftwaretestingandcodereviewprojects,supportingclientorganizations inthetechnology,defense,andfinanceindustries,aswellasgovernmententities.Notable clientsincludeHashiCorp,Google,Microsoft,WesternDigital,andZoom. hasheyealsooperatesacenterofexcellencewithregardtoblockchainsecurity.Notable projectsincludeauditsofAlgorand,BitcoinSV,Chainlink,Compound,Ethereum2.0, MakerDAO,Matic,Uniswap,Web3,andZcash. Tokeepuptodatewithourlatestnewsandannouncements,pleasefollowhasheyeon Twitterandexploreourpublicrepositoriesathttps://github.com/hasheye-io.Toengageus directly,visitour"Contact"pageathttps://www.hasheye.io/contact,oremailusat info@hasheye.io. hasheye,Inc. 497CarrollSt.,Space71,SeventhFloor Brooklyn,NY11215 https://www.hasheye.io info@hasheye.io hasheye 1ULTI PUBLIC SecurityAssessment

NoticesandRemarks CopyrightandDistribution ©2024byhasheye,Inc. Allrightsreserved.hasheyeherebyassertsitsrighttobeidentifiedasthecreatorofthis reportintheUnitedKingdom. Thisreportisconsideredbyhasheyetobepublicinformation;itislicensedtoULTI underthetermsoftheprojectstatementofworkandhasbeenmadepublicatULTI's request.Materialwithinthisreportmaynotbereproducedordistributedinpartorin wholewithouttheexpresswrittenpermissionofhasheye. Thesolecanonicalsourceforhasheyepublicationsisthehasheyepublicationspage. Reportsaccessedthroughanysourceotherthanthatpagemayhavebeenmodifiedand shouldnotbeconsideredauthentic. TestCoverageDisclaimer Allactivitiesundertakenbyhasheyeinassociationwiththisprojectwereperformedin accordancewithastatementofworkandagreeduponprojectplan. Securityassessmentprojectsaretime-boxedandoftenreliantoninformationthatmaybe providedbyaclient,itsaffiliates,oritspartners.Asaresult,thefindingsdocumentedin thisreportshouldnotbeconsideredacomprehensivelistofsecurityissues,flaws,or defectsinthetargetsystemorcodebase. hasheyeusesautomatedtestingtechniquestorapidlytestthecontrolsandsecurity propertiesofsoftware.Thesetechniquesaugmentourmanualsecurityreviewwork,but eachhasitslimitations:forexample,atoolmaynotgeneratearandomedgecasethat violatesapropertyormaynotfullycompleteitsanalysisduringtheallottedtime.Theiruse isalsolimitedbythetimeandresourceconstraintsofaproject. hasheye 2ULTI PUBLIC SecurityAssessment

 hasheye 3ULTI PUBLIC SecurityAssessment

ProjectSummary ContactInformation Thefollowingprojectmanagerwasassociatedwiththisproject: SamGreenup,ProjectManager sam.greenup@hasheye.io Thefollowingengineeringdirectorwasassociatedwiththisproject: JosselinFeist,EngineeringDirector,Blockchain josselin.feist@hasheye.io Thefollowingconsultantwasassociatedwiththisproject: ElvisSkoždopolj,Consultant elvis.skozdopolj@hasheye.io ProjectTimeline Thesignificanteventsandmilestonesoftheprojectarelistedbelow. DateEvent December13,2024Pre-projectkickoffcall December20,2024Deliveryofreportdraft December20,2024Reportreadoutmeeting December23,2024Completionoffixreview December27,2024Deliveryoffinalsummaryreport hasheye 4ULTI PUBLIC SecurityAssessment

ProjectTargets Theengagementinvolvedareviewandtestingofthefollowingtarget. ULTISmartContracts Repositoryhttps://github.com/ulti-org/ulti-protocol-contract Version a03dd8890760ea2c517858fe35461619ccf58110 TypeSolidity PlatformEthereum hasheye 5ULTI PUBLIC SecurityAssessment

ExecutiveSummary EngagementOverview ULTIengagedhasheyetoreviewthesecurityoftheULTIsmartcontracts.ULTIisan incentivizedsavingsprotocolthroughwhichusersacquireULTItokens.ULTIcreatesa Uniswapv3positionconsistingoftheULTItokenandtheinput/underlyingtoken.Users depositingintotheprotocolgetacertainamountofULTImintedtothemdependingonthe currenttime-weightedaverageprice(TWAP)ratiointheUniswappool,andareincentivized tokeepdepositingviathestreak,referral,andtopcontributorbonuses.Topcontributors areabletocallapermissionedfunctiontoswapthereservesoftheunderlyingtokenfor ULTI. Oneconsultantconductedthereviewfrom December16toDecember20,2024,foratotal ofoneengineer-weekofeffort.Withfullaccesstosourcecodeanddocumentation,we performedstaticanddynamictestingofthecodebase,usingautomatedandmanual processes. ObservationsandImpact TheULTIsystemconsistsofthreesmartcontracts:themain ULTI contract,the ULTIData contract,whichcontainsfunctionsmeanttobecalledoff-chain,andthe ULTIShared library,whichcontainstheconstants.Thefocusofthisreviewwasthemain ULTI contract. Wereviewedthedepositandclaimflow,lookingforwaysinwhichuserscouldincrease theirULTIallocation,waysinwhichuserscoulddecreaseanotheruser’sallocation, arithmeticandroundingissues,andMEVrisks.Wereviewedhowreferralsand contributionsareaccountedfortoinvestigatewhetheritispossibletolooporchain referralsinordertogainalargerULTIbonus,whetherreferralscanbecanceledor replaced,whetheraccountingvaluesareproperlyremovedwhenatopcontributoris deleted,whetheratopcontributorcanbeunfairlyremovedoradded,andwhetherthe claimdelayscanbeavoided.Thelibrarycontractsinthe lib/uniswap directoryarecopies oftheUniswapv3librarieswithsomeminormodifications.Wecomparedtheselibraries againsttheoriginalimplementationanddifferentiallyfuzzedthe FullMath libraryusing Foundry.Thedeploymentscriptswereconsideredoutofscopeforthisreview. Wediscoveredoneinformational-severityfindinginthemodificationsmadetothe FullMath functionandonelow-severityfindingrelatedtoinconsistentprecisionwhen mintingULTI,whichcouldresultinlessULTIbeingminted.WealsofoundthattheUniswap reentrancylockcanbeusedtoforceasilentfailureofthe _tryIncreaseLiquidity functionbyreenteringintothe ULTI contract’s deposit functionfromaswapormint callback,keepingtheinputtokeninthe ULTI contract.However,thisdoesnotpresenta clearsecurityissueatthistime,soitisnotdisclosedasafindinginthisreport. hasheye 6ULTI PUBLIC SecurityAssessment

Additionally,wenotedseveralcodequalityissues;addressingthemwouldimprovethe codereadabilityandmaintainability. Recommendations Basedonthecodebasematurityevaluationandfindingsidentifiedduringthesecurity review,hasheyerecommendsthatULTItakethefollowingsteps: • Remediatethefindingsdisclosedinthisreport.Thesefindingsshouldbe addressedaspartofadirectremediationoraspartofanyrefactorthatmayoccur whenaddressingotherrecommendations. • Implementathoroughfuzzingharness.Thesystemimplementslargedelays(e.g., thebonusclaimdelay,whichis99days),reliesoninteractionswithaUniswappool, andrequiresatleast33topcontributorsbeforetopcontributorsaresorted.Testing theprotocolforalongertimeperiod(i.e.,simulatingtimepassingviafuzzing)will helptoconfirmthattheprotocolbehavesasexpectedwhenallfeaturesareactive. hasheye 7ULTI PUBLIC SecurityAssessment

CodebaseMaturityEvaluation hasheyeusesatraffic-lightprotocoltoprovideeachclientwithaclearunderstandingof theareasinwhichitscodebaseismature,immature,orunderdeveloped.Deficiencies identifiedhereoftenstemfromrootcauseswithinthesoftwaredevelopmentlifecyclethat shouldbeaddressedthroughstandardizationmeasures(e.g.,theuseofcommonlibraries, functions,orframeworks)ortrainingandawarenessprograms. CategorySummaryResult ArithmeticThearithmeticformulasarestraightforward,mostly dealingwithpriceconversionandpercentage calculations.Allarithmeticformulasarethoroughly documentedinthecode.Uncheckedarithmeticisused onlyinthemodifiedthird-partylibraries.However,we diddiscoveroneissueinwhichuncheckedarithmetic shouldbeused(finding2),andULTIcouldbenefitfrom moreconsistencyinthearithmeticprecisionandthe selectionofscalingfactors(finding1). Moderate AuditingMoststate-changingfunctionsemitevents,although having _updateTopContributors emitaneventwould bebeneficialtomonitorthecorrectreplacementoftop contributors.Wearenotawareofanincidentresponse

planormonitoringstrategy;however,thesystemisfully decentralized,andtheownerhasnopowertomodifyit afteritisdeployed.Duetothisdecentralization, monitoringisnotasimportantforthisparticularsystem. Satisfactory Authentication/ AccessControls The ULTI contractcontainsonlytwopermissioned functions,onefortheowner,whichisusedonlyonceto launchthesystem,andoneforthetopcontributors.No accesscontrolissueswerefound.Thesystemisfully decentralized. Satisfactory Complexity Management Thesystemconsistsofonlyonemainsmartcontractand twoutilitycontracts.Thecontractsandlibrariesusedby thesystemareinheritedfromUniswapand OpenZeppelinorarecopiedandmodifiedfromUniswap. TheAPIislimited,withonlyacoupleofactionsavailable tousers.Themostcomplexpartsofthesystemarethe interactionsofthereferral,streak,andcontributor Satisfactory hasheye 8ULTI PUBLIC SecurityAssessment

bonuses.Selectingasinglescalingfactorforarithmetic calculationswouldhelpreducesomecomplexityofthe arithmetic. DecentralizationThesystemisfullydecentralizedafterlaunch.Theowner isonlyabletolaunchthesystem,afterwhichthe ownershipisrenounced.Theonlyotherprivilegedrole, theguardians,isselectedbasedoncontributionstothe protocol. Strong DocumentationTheprotocolhasstrongdocumentationintheformofa litepaper,awhitepaper,andveryextensiveinlinecode andNatSpecdocumentation.Itwouldbebeneficialto createadditionalinternaldocumentationdetailingthe possiblescenariosinwhichthe pump functionmightnot workormightleadtolargerslippage. Strong Low-Level Manipulation Thesystemdoesnotuselow-levelmanipulationexcept inthemodifiedthird-partylibrarycontracts. Satisfactory Testingand Verification Thecodebasehasunittestswritteninjavascriptthat covermostexpectedscenarios.Thetestingsuitedoes nottestinteractionswiththeUniswappooloutsidethe protocol.Defininginvariantsandtestingthemusing smartcontractfuzzingwouldbebeneficialinorderto confirmthesystembehavesasexpectedunderheavy load,duringexternalinteractionswiththeUniswappool, andafterthepredefineddelayshavepassed. Thetestingsuitewasonlybrieflyreviewed;thisarea requiresadditionalinvestigation. Further Investigation Required Transaction Ordering Thesystemispotentiallysusceptibletomevrisks; however,theserisksseemtobeproperlymitigatedvia theuseofslippageparameters. Satisfactory hasheye 9ULTI PUBLIC SecurityAssessment

SummaryofFindings Thetablebelowsummarizesthefindingsofthereview,includingtypeandseveritydetails. IDTitleTypeSeverity 1UserscanreceivelessULTIfordepositsdueto precisionloss Data Validation Low 2MissinguncheckedblockinFullMathData Validation Informational hasheye 10ULTI PUBLIC SecurityAssessment

A.VulnerabilityCategories
Thefollowingtablesdescribethevulnerabilitycategories,severitylevels,anddifficulty levelsusedinthisdocument. VulnerabilityCategories CategoryDescription AccessControlsInsufficientauthorizationorassessmentofrights AuditingandLoggingInsufficientauditingofactionsorloggingofproblems AuthenticationImproperidentificationofusers ConfigurationMisconfiguredservers,devices,orsoftwarecomponents CryptographyAbreachofsystemconfidentialityorintegrity DataExposureExposureofsensitiveinformation DataValidationImproperrelianceonthestructureorvaluesofdata DenialofServiceAsystemfailurewithanavailabilityimpact ErrorReportingInsecureorinsufficientreportingoferrorconditions PatchingUseofanoutdatedsoftwarepackageorlibrary SessionManagementImproperidentificationofauthenticatedusers TestingInsufficienttestmethodologyortestcoverage TimingRaceconditionsorotherorder-of-operationsflaws UndefinedBehaviorUndefinedbehaviortriggeredwithinthesystem hasheye 11ULTI PUBLIC SecurityAssessment

SeverityLevels SeverityDescription
InformationalTheissuedoesnotposeanimmediateriskbutisrelevanttosecuritybest practices.
UndeterminedTheextentoftheriskwasnotdeterminedduringthisengagement.
LowTheriskissmallorisnotonetheclienthasindicatedisimportant.
MediumUserinformationisatrisk;exploitationcouldposereputational,legal,or moderatefinancialrisks.
HighTheflawcouldaffectnumeroususersandhaveseriousreputational,legal, orfinancialimplications.
DifficultyLevels DifficultyDescription
UndeterminedThedifficultyofexploitationwasnotdeterminedduringthisengagement.
LowTheflawiswellknown;publictoolsforitsexploitationexistorcanbe scripted.
MediumAnattackermustwriteanexploitorwillneedin-depthknowledgeofthe system.
HighAnattackermusthaveprivilegedaccesstothesystem,mayneedtoknow complextechnicaldetails,ormustdiscoverotherweaknessestoexploitthis issue. hasheye 12ULTI PUBLIC SecurityAssessment

B.CodeMaturityCategories
Thefollowingtablesdescribethecodematuritycategoriesandratingcriteriausedinthis document.

CodeMaturityCategories CategoryDescription
ArithmeticTheproperuseofmathematicaloperationsandsemantics
AuditingTheuseofeventauditingandloggingtosupportmonitoring Authentication/ AccessControls
Theuseofrobustaccesscontrolstohandleidentificationand
authorizationandtoensuresafeinteractionswiththesystem Complexity Management
Thepresenceofclearstructuresdesignedtomanagesystemcomplexity,
includingtheseparationofsystemlogicintoclearlydefinedfunctions
DecentralizationThepresenceofadecentralizedgovernancestructureformitigating
insiderthreatsandmanagingrisksposedbycontractupgrades
DocumentationThepresenceofcomprehensiveandreadablecodebasedocumentation Low-Level Manipulation
Thejustifieduseofinlineassemblyandlow-levelcalls Testingand Verification
Thepresenceofrobusttestingprocedures(e.g.,unittests,integration
tests,andverificationmethods)andsufficienttestcoverage Transaction Ordering
Thesystem’sresistancetotransaction-orderingattacks RatingCriteria RatingDescription
StrongNoissueswerefound,andthesystemexceedsindustrystandards.
SatisfactoryMinorissueswerefound,butthesystemiscompliantwithbestpractices.
ModerateSomeissuesthatmayaffectsystemsafetywerefound.
WeakManyissuesthataffectsystemsafetywerefound.
MissingArequiredcomponentismissing,significantlyaffectingsystemsafety. hasheye 13ULTI PUBLIC
SecurityAssessment

NotApplicableThecategoryisnotapplicabletothisreview.
NotConsideredThecategorywasnotconsideredinthisreview. Further Investigation Required
Furtherinvestigationisrequiredtoreachameaningfulconclusion. hasheye 14ULTI PUBLIC
SecurityAssessment

C.CodeQualityFindings
Thefollowingfindingsarenotassociatedwithspecificvulnerabilities.However,addressing
themmayenhancecodereadabilityandmaypreventtheintroductionofvulnerabilitiesin thefuture. ●
Thecodebaseusesanumberofdifferentscalingfactorsanddenominators
dependingonthecalculationsperformed.Thiscreatesunnecessarycognitive
overheadandmakesthecodebasehardertoreviewandmaintain.Werecommend
thatasingleprecisionfactoranddenominatorbechosenandusedforcalculations throughoutthecodebase. ● The
name and symbol variablesusedinthe ULTI contract’sconstructorshadowthe ERC-
20statevariables.Thevariablesshouldberenamedinordertoavoidvariable nameshadowing. ● The
nextDepositOrClaimTimestamp mappingischeckedtwiceinthe _deposit
function.Thesecondoccurrencecanbesafelyremovedsinceitwasalreadychecked intheif-revertstatement.
if(block.timestamp<nextDepositOrClaimTimestamp[msg.sender])revert DepositCooldownActive();
//2.Auto-claimpendingULTIifrequested boolautoClaimed;
if(autoClaim&&block.timestamp≥nextDepositOrClaimTimestamp[msg.sender]&&
claimableUlti[msg.sender]>0){ FigureC.1: ULTI.sol#L894-L898 ● The maxBonusPlusOne
localvariableistheresultofanexpressionusingonly
constantsandliterals.Thisexpressioncanberewrittenasaconstant. uint256maxBonusPlusOne=
(ULTIShared.STREAK_BONUS_MAX_PERCENTAGE+1)* ULTIShared.PRECISION_FACTOR_1E6/100;//0.34scaledby1e6
FigureC.2: ULTI.sol#L1593 ● Anumberofconstantsareassignedtotheresultofanexpressionthatusesother
constants.Thistypeofconstantisevaluatedatruntimeinsteadoftheresultbeing
savedinbytecode,resultinginaslightlyhighergascost.Theconstantscanbe
precomputedanddirectlyassignedtoavalueinordertoreducethegascosts.
///@noticeCycleintervalinseconds(33days) uint256publicconstantCYCLE_INTERVAL=(ULTI_NUMBER*1days);
hasheye 15ULTI PUBLIC SecurityAssessment

///@noticeMinimumtimeintervalforTime-WeightedAveragePrice(TWAP)calculation (18minutesand9seconds)
uint32publicconstantMIN_TWAP_INTERVAL=uint32((ULTI_NUMBER*33seconds));
///@noticeIntervalbetweenallbonusesclaims(99days) uint256publicconstantALL_BONUSES_CLAIM_INTERVAL=
(ULTI_NUMBER*3days); //Liquiditypoolconstants
///@noticePercentageofcontributionsallocatedtoliquiditypool
uint256publicconstantLP_CONTRIBUTION_PERCENTAGE=ULTI_NUMBER/11;//3%
///@noticeMaximumallowedslippageforaddingliquidityinbasispoints:99BPS (0.99%)
uint256publicconstantMAX_ADD_LP_SLIPPAGE_BPS=3*ULTI_NUMBER;
///@noticeMaximumallowedslippageforswapsinbasispoints:132BPS(1.32%)
uint256publicconstantMAX_SWAP_SLIPPAGE_BPS=4*ULTI_NUMBER; //Bonus-relatedconstants
///@noticePercentageofcontributionsallocatedtotopcontributors
uint256publicconstantTOP_CONTRIBUTOR_BONUS_PERCENTAGE=ULTI_NUMBER/11;//3%
///@noticeIntervalbetweenpumpactions:3300seconds(55minutes) uint256publicconstantPUMP_INTERVAL=
(ULTI_NUMBER*100seconds); ///@noticeMinimumnumberofpumpsrequiredtobeclassifiedasanactivepumper
uint256publicconstantMIN_PUMPS_FOR_ACTIVE_PUMPERS=ULTI_NUMBER/3;

///@noticeMaximumnumberofpumpsallowedperuserpercycle(33)
uint256publicconstantMAX_PUMPS_FOR_ACTIVE_PUMPERS=ULTI_NUMBER;
///@noticePercentagebonusforactivepumpers(3%ofthetopcontributorbonus)
uint256publicconstantACTIVE_PUMPERS_BONUS_PERCENTAGE=ULTI_NUMBER/10; FigureC.3: ULTIShared.sol • The inputTokenDecimals statevariableissetintheconstructorbutisneverused. Itcanberemoved. • The _isTopContributor functionofthe ULTIData contractfetchesalistof contributorsandloopsoveritinordertodeterminewhethertheuseraddressisa partofthelist.Sincethe topContributors mappingisan EnumerableMap type, thisinformationcanbemoreeasilyfetchedbyusingthe contains function. • The _isActivePumper functionofthe ULTI contractcouldbemadepublicinorder toavoidhavingtoreimplementitinthe ULTIData contract. • The depositedInCurrentCycle variablecouldberemovedandthecheckcould beperformeddirectlyinthe if statement,sincethevariableisusedonlyonce. hasheye 16ULTI PUBLIC SecurityAssessment

booldepositedInCurrentCycle=currentCycleDeposits>0; if(!depositedInCurrentCycle){ streakCount=ulti.streakCounts(cycle-1,user); } FigureC.4: ULTIData.sol#L238-L241 • The _updateTopContributors functionshouldemitaneventwhenanew contributorisaddedorapreviouscontributorisremovedfromtheset.Thiswill helpwithmonitoringthecontractforunexpectedbehavior. • The getUserData functionofthe ULTIData contractreturnszeroastheminimum boundinsteadoftheactualminimumforthefirstcycle.Thisshouldbefixed. hasheye 17ULTI PUBLIC SecurityAssessment

D.FixReviewResults Whenundertakingafixreview,hasheyereviewsthefixesimplementedforissues identifiedintheoriginalreport.Thisworkinvolvesareviewofspecificareasofthesource codeandsystemconfiguration,notcomprehensiveanalysisofthesystem.
OnDecember23,2024,hasheyereviewedthefixesandmitigationsimplementedbythe ULTIteamfortheissuesidentifiedinthisreport.Wereviewedeachfixtodetermineits effectivenessinresolvingtheassociatedissue.
Insummary,ULTIhasresolvedbothoftheissuesdisclosedinthisreport.Foradditional information,pleaseseetheDetailedFixReviewResultsbelow. IDTitleSeverityStatus 1UserscanreceivelessULTIfordepositsdueto precisionloss LowResolved 2MissinguncheckedblockinFullMathInformationalResolved DetailedFixReviewResults TOB-ULTI-1:UserscanreceivelessULTIfordepositsduetoprecisionloss Resolvedincommit 579d372 .Theorderofoperationsinthe _allocateDeposit function’sarithmeticwasupdatedtoperformmultiplicationbeforedivisioninorderto preservetheprecisionoftheoperation. TOB-ULTI-2:MissinguncheckedblockinFullMath Resolvedincommit 648f79f .Uncheckedarithmeticwasaddedtothe FullMath library’s mulDiv function. hasheye 18ULTI PUBLIC SecurityAssessment

E.FixReviewStatusCategories
Thefollowingtabledescribesthestatusesusedtoindicatewhetheranissuehasbeen sufficientlyaddressed.
FixStatus StatusDescription UndeterminedThestatusoftheissuewasnotdeterminedduringthisengagement.
UnresolvedTheissuepersistsandhasnotbeenresolved.
PartiallyResolvedTheissuepersistsbuthasbeenpartiallyresolved.
ResolvedTheissuehasbeensufficientlyresolved. hasheye 19ULTI PUBLIC SecurityAssessment