HashEye

// SMART CONTRACT SECURITY AUDIT

Elixir Protocol

Security assessment by HashEye · prepared for Elixir Technologies Ltd

HASHEYE AUDITED

PROJECT	Elixir Protocol
CLIENT	Elixir Technologies Ltd
CATEGORY	Blockchain
PUBLISHED	August 1, 2024
REPORT ID	research-elixir-protocol-2024-08-01-fhk6ur

This report was produced under HashEye's layered review process — **automated detection**, **pattern correlation**, and **senior manual verification** — with every finding signed off by a human reviewer. Full findings detail and on-chain attestation are available on the report page at hasheye.io/audits/research-elixir-protocol-2024-08-01-fhk6ur.

ElixirProtocol SecurityAssessment October10,2024 Preparedfor: ChrisGilbert ElixirTechnologiesLtd. Preparedby:ArturCygan,DamilolaEdwards,BoHenderson,andEmilioLópez

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 1ElixirProtocolSecurityAssessment PUBLIC

NoticesandRemarks CopyrightandDistribution ©2024byhasheye,Inc. Allrightsreserved.hasheyeherebyassertsitsrighttobeidentifiedasthecreatorofthis reportintheUnitedKingdom. Thisreportisconsideredbyhasheyetobepublicinformation;itislicensedtoElixir TechnologiesLtdunderthetermsoftheprojectstatementofworkandhasbeenmade publicatElixirTechnologiesLtd'srequest.Materialwithinthisreportmaynotbe reproducedordistributedinpartorinwholewithouttheexpresswrittenpermissionof hasheye. 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 2ElixirProtocolSecurityAssessment PUBLIC

TableofContents

16.Responsepayloadtoauthenticationchallengeisnotsigned43
17.APIdoesnotvalidatedisplay_nameandapp_version44 18.Allon-chaineventsreplayeduponstartup45
19.RedpandaexposedtotheInternet47 20.APIhasadminaccesstoRedpanda48 21.Useofunpinnedthird-
partyDockerimagesandactionsonworkflows50 hasheye 3ElixirProtocolSecurityAssessment PUBLIC

22.AbsenceofaccesscontrolsonpoolcreationfunctionA.VulnerabilityCategories54
B.CodeMaturityCategories56 C.CodeQualityRecommendations58 D.AutomatedAnalysisToolConfiguration61
E.MutationTesting63 F.IncidentResponseRecommendations65
G.SecurityBestPracticesforUsingMultisignatureWallets67 H.FixReviewResults69
DetailedFixReviewResults71 I.FixReviewStatusCategories74 hasheye 4ElixirProtocolSecurityAssessment
PUBLIC

ProjectSummary ContactInformation Thefollowingprojectmanagerwasassociatedwiththisproject:
SamGreenup,ProjectManager sam.greenup@hasheye.io
Thefollowingengineeringdirectorwasassociatedwiththisproject:
KeithHoodlet,EngineeringDirector,ApplicationSecurity keith.hoodlet@hasheye.io
JosselinFeist,EngineeringDirector,Blockchain josselin@hasheye.io
Thefollowingconsultantswereassociatedwiththisproject:
ArturCygan,ConsultantDamilolaEdwards,Consultant artur.cygan@hasheye.iodamilola.edwards@hasheye.io
BoHenderson,ConsultantEmilioLópez,Consultant bo.henderson@hasheye.ioemilio.lopez@hasheye.io
ProjectTimeline Thesignificanteventsandmilestonesoftheprojectarelistedbelow. DateEvent
July24,2024Pre-projectkickoffcall August2,2024Statusupdatemeeting#1
August9,2024Deliveryofreportdraft August9,2024Reportreadoutmeeting
October10,2024Deliveryofcomprehensivereport hasheye 5ElixirProtocolSecurityAssessment PUBLIC

ExecutiveSummary EngagementOverview
ElixirTechnologiesLtdengagedhasheyetoreviewthesecurityofElixirProtocol.Elixiris aconsensus-
basedpeer-to-peernetworkingprotocolthatperformsalgorithmictradeson
centralizedanddecentralizedexchanges.
AteamoffourconsultantsconductedthereviewfromJuly29toAugust7,2024,foratotal offiveengineer-
weeksofeffort.Ourtestingeffortsfocusedonthestakinganddelegation
methodsofthesmartcontracts,userauthentication,andsoundnessoftheconsensus
mechanism.Withfullaccesstosourcecodeanddocumentation,weperformedstaticand dynamictestingofthe
elixir-protocol and elixir-protocol-api repositories,using automatedandmanualprocesses.
ObservationsandImpact OurreviewofElixirProtocoluncoveredseveralhigh-
severityissues,althoughmostarealso highlydifficulttoexploit.However,onehigh-
severityissuerequiresonlylowdifficultyto
exploit;thisissueallowsdelegatorstobypasstheredelegatecooldownperiod (TOB-ELIXIR-
12)byimmediatelysignalingaftertheinitialdelegation.Othernoteworthy
findingsincludealackofdatavalidationthatenablesthestrategyexecutortosignarbitrary
payloadsprovidedbytheAPI(TOB-ELIXIR-6).
Weidentifiedtwoissuesrelatingtotheconsensusmechanism.Onerelatestoinadequate
deauthorizationofuserswhowerepreviouslyinthesetofcorevalidators,allowing
minorityvalidatorstoparticipateinconsensus(TOB-ELIXIR-13).Asecondissueinthe
quorumrequirementcouldcausetheconsensusmechanismtohaltifthequeueofactive, non-
corevalidatorsgrowstoolarge(TOB-ELIXIR-14).
ThesystemexposesRedpandatotheinternet;thisdesigndecisionledtoseveralfindings (TOB-ELIXIR-9,TOB-
ELIXIR-19,andTOB-ELIXIR-20). Allinall,thecodebaseiswell-
organizedandfeaturesthoroughcodecomments,which
aidedoursecurityreview.However,thesystemneedstobetestedmorethoroughlyprior
todeployment.Someissues,suchasanincorrectcalculationoftheminimumproposal
requirementinthemajoritygroup(TOB-ELIXIR-4),couldhavebeencaughtearlierbymore thoroughunittests.
Recommendations Basedonthecodebasematurityevaluationandfindingsidentifiedduringthesecurity
review,hasheyerecommendsthatElixirTechnologiesLtdtakethefollowingsteps
beforedeployingtheprotocoltoproduction: hasheye 6ElixirProtocolSecurityAssessment PUBLIC

• Remediatethefindingsdisclosedinthisreport.Thesefindingsshouldbe
addressedaspartofadirectremediationoraspartofanyrefactorthatmayoccur
whenaddressingotherrecommendations. •
Expandthetestsuite.Weidentifiedgapsinthesmartcontracttestcoverageusing
mutationtests.Writeadditionaltestsbthatasserttheexpectedbehaviorofevery
branchofthebusinesslogic,andthenusecodecoverageassessmentstoconfirm
thatgapsintestcoveragehavebeenclosed. • Writedocumentation.Althoughthecodeiswellcommented,high-
level documentationisnecessarytoensurethatendusers cansafelyinteractwithElixir protocol. ○
Writegoal-orientedusagemanuals,oneforeachtypeofenduser(e.g.,
staker,validator,trader).Theseshouldprovideclearhow-toinstructionsthat

guideusersthrougheveryactiontheymightneedtotakeandshouldclearly outlinetherisksassociatedwithanygivenactionwithaccompanying guidanceonmitigatingoreliminatingtheserisks. ○ CreateanAPIreferencethatdocumentsallsmartcontractmethodsandAPI endpoints.Theparameters,returnvalues,andsideeffectsshouldbelistedin oneplacethatiseasytosearch.Inaddition,interactionsbetween componentsshouldbedescribedtocomplementtheexistingsystem diagrams.Thiswillhelpcurrentdevelopersaddnewfeaturessafely,aid futuredevelopersinrampingupquickly,andhelpothersecurityreviewersto assessthecodebaseproductively. ○ Createanincidentresponseplan.SeeappendixFforguidance. • Assignownershiptoamultisignaturewallet.Contractupgradesareextremely sensitiveoperationsanddonotrequirefrequentorautomatedexecution,so multisignaturewalletswouldbeagoodfitforownershiprolesthatcanauthorize upgrades.SeeappendixGforguidanceregardingthesecureusageof multisignaturewallets. hasheye 7ElixirProtocolSecurityAssessment PUBLIC

FindingSeveritiesandCategories Thefollowingtablesprovidethenumberoffindingsbyseverityandcategory. EXPOSUREANALYSIS SeverityCount High8 Medium4 Low2 Informational5 Undetermined3 CATEGORYBREAKDOWN CategoryCount AccessControls2 Configuration4 Cryptography1 DataExposure1 DataValidation7 DenialofService4 Patching1 SessionManagement1 Timing1 hasheye 8ElixirProtocolSecurityAssessment PUBLIC

ProjectGoals TheengagementwasscopedtoprovideasecurityassessmentoftheElixirProtocol. Specifically,wesoughttoanswerthefollowingnon-exhaustivelistofquestions: • Arethereanyerror-proneorincorrectstepsinthedeploymentandinitializationof thesystem’ssmartcontracts? • Isthereanywayforausertobypasstheredelegateandunstakecooldownperiods? • Doesoff-chaincodemanagekeys,usecryptographicprimitives,andinteractwith smartcontractssafely? • Couldanattackerstealfromusersordenythemaccesstotheirstakedfunds? • Isalluser-providedinputproperlyvalidated? • Cananattackercaptureorhaltthesystem’sconsensusmechanism? • Areanyaccesscontrolsmissing,anddoanyroleshaveunsuitablepermissions? • Cananysystemactionsbefront-run,orarethereotherraceconditionsthatan attackercouldtakeadvantageof? hasheye 9ElixirProtocolSecurityAssessment PUBLIC

ProjectTargets Theengagementinvolvedareviewandtestingofthetargetslistedbelow. protocol Repository https://github.com/ElixirProtocol/elixir-protocol Version 99e669d6a1cd88011a395fc74cf374372f8b5c52 TypePython,Solidity PlatformEVM,Linux protocol-api Repository https://github.com/ElixirProtocol/elixir-protocol-api Version f508fc1a120886688da020f55dd22dbb0f303ccd TypePython PlatformLinux hasheye 10ElixirProtocolSecurityAssessment PUBLIC

ProjectCoverage Thissectionprovidesanoverviewoftheanalysiscoverageofthereview,asdeterminedby ourhigh-levelengagementgoals.Ourapproachesincludedthefollowing: • Smartcontracts.Weranslitherandslither-mutatetoautomaticallyidentifypoints ofinterestandgapsinthetestcoveragetoguideourmanualreview. ○ Core :Apermissionedactorthatcontrolsadministrativefunctionssuchas settingimportantaddressesandslashingusers.Wereviewedthe initializationprocess,accesscontrols,andthiscontract’sinteractionswith othercomponents. ○ DisputeManager :Thiscontractallowsanyonewithavalid ConsensusAuditDetails structtotriggerthejailingofmisbehaving validators.Wereviewedthesignaturevalidationlogicandaddresschecksto assesswhetherinvalidparameterscanbeusedtopreventjailingadishonest validatorortocauseanhonestactortobejailed. ○ Pool and PoolManager :Thesecontractsactasanauditablerecordofall poolsandtheirconfigurationparameters.Sincethesecomponentscontain littlelogic,wespentlesstimereviewingthembeyonddeterminingif initializationandownershipmethodsbehaveasexpected. ○ StakeManager :Thiscontractcontainscriticalmethodsthattiedirectlyinto theconsensusmechanismandwastheprimaryfocusofoursmartcontract review.Weassessedthemovementoffundsintoandoutofthecontract, lookingforopportunitiestostealorlockuserfunds.Welistedthedifferent contractstatesandtransitionsbetweenthemtoidentifywaysthatauser couldbypassthesignaldelays,delegatemorethantheystaked,orotherwise disruptthesystem. • Protocolservices.ThesePythonmodulesimplementthecoreoff-chainbusiness logicoftheElixirprotocol.Thetwoserviceswelookedatmostcloselyarethe following: ○ Consensusprocessor:Welookedforwaysthatanattackercouldabuse delegationsorperformsybilattackstodisrupttheconsensusbuilding

process.Wereviewedthearithmeticsupportingvalidatorandproposal countsalongwiththeoverallbusinesslogicsearchingforwaysthatan attackercouldcaptureorhaltconsensus. hasheye 11ElixirProtocolSecurityAssessment PUBLIC

○ Strategyexecutor:Thiscomponentingestsdataframesandproducesorder proposals.Wereviewedthestrategyexecutorpayingparticularattentionto itsauthorizationwiththeprotocolapi. ● ProtocolAPI:The protocol-api managesuserauthenticationandactsasa gatewayforinteractionswithancillaryRedisanddatabaseservices.Wesearchedfor waysthatauthenticationcouldbebypassedandcarefullystudiedthiscomponent's interactionswiththeconsensusservice. CoverageLimitations Becauseofthetime-boxednatureoftestingwork,itiscommontoencountercoverage limitations.Thefollowinglistoutlinesthecoveragelimitationsoftheengagementand indicatessystemelementsthatmaywarrantfurtherreview: ● Weperformedonlyautomatedanalysisandlightmanualreviewoftheprotocol servicesthatwerenotexplicitlylistedabove. ● TheorderproposalgenerationandGLTstrategycodewasnotaprimaryfocusof ourreview. ● Wedidnotthoroughlyreviewfilesmanagingtheproductionenvironmentsuchas Dockerfilesandothercloudconfigfiles. hasheye 12ElixirProtocolSecurityAssessment PUBLIC

AutomatedTesting hasheyeusesautomatedtechniquestoextensivelytestthesecuritypropertiesof software.Weusebothopen-sourcestaticanalysisandfuzzingutilities,alongwithtools developedinhouse,toperformautomatedtestingofsourcecodeandcompiledsoftware. TestHarnessConfiguration Weusedthefollowingtoolsintheautomatedtestingphaseofthisproject: ToolDescriptionPolicy SlitherAstaticanalysisframeworkthatcanstaticallyverify algebraicrelationshipsbetweenSolidityvariables AppendixD slither-mutate Adeterministicmutationgeneratorthatdetectsgaps intestcoverage AppendixE SemgrepAnopen-sourcestaticanalysistoolforfindingbugs andenforcingcodestandardswheneditingor committingcodeandduringbuildtime AppendixD BanditAstaticanalysistooldesignedtofindcommon securityissuesinPythoncode AppendixD CodeQLAcodeanalysisenginedevelopedbyGitHubto automatesecuritychecks AppendixD AreasofFocus Ourautomatedtestingandverificationworkfocusedonthefollowingsystemproperties: ● IdentifycommonissuesandAnti-patternsinSolidityandPython ● Identifygapsintestcoveragetoguideourreviewefforts TestResults Theresultsofthisfocusedtestingaredetailedbelow. hasheye 13ElixirProtocolSecurityAssessment PUBLIC

slither-mutate :Thefollowingtabledisplaystheportionofeachtypeofmutantfor whichallunittestspassed.Thepresenceofvalidmutantsindicatesthattherearegapsin testcoveragebecausethetestsuitedidnotcatchtheintroducedchange. ● Uncaughtrevertmutantsreplaceagivenexpressionwitha revert statementand indicatethatthelineisnotexecutedduringtesting. ● UncaughtcommentmutantscommentoutagivenexpressionandindicatethatthE effectsofthislinearenotcheckedbyanyassertions. ● Uncaughttweakmutantsindicatethattheexpressionbeingexecutedfeaturesedge casesthatarenotcoveredbythetestsuite. The protocol/contracts/src subdirectoryistherootforalltargetpathslistedbelow. Contractssupportingtestsorthatproducedzeroanalyzedmutants(e.g.,interfaces)were omittedfrommutationtestinganalysis. TargetUncaught Reverts Uncaught Comments Uncaught Tweaks ELX.sol 100%100%100% Pool.sol 0%42%14% PoolManager.sol 11%50%N/A StakeManager.sol 0%22%11% Core.sol 24%45%32% DisputeManager.sol 0%29%0% hasheye 14ElixirProtocolSecurityAssessment PUBLIC

CodebaseMaturityEvaluation hasheyeusesatraffic-lightprotocoltoprovideeachclientwithaclearunderstandingof theareasinwhichitscodebaseismature,immature,orunderdeveloped.Deficiencies identifiedhereoftenstemfromrootcauseswithinthesoftwaredevelopmentlifecyclethat shouldbeaddressedthroughstandardizationmeasures(e.g.,theuseofcommonlibraries, functions,orframeworks)ortrainingandawarenessprograms. CategorySummaryResult ArithmeticTheprotocolusesamodernversionofSolidityWithout anyuncheckedarithmeticblocks,preventingoverflows. Smartcontractarithmeticusesonlysimpleadditionand subtraction,eliminatingthepossibilityofissuesdueto roundingerrors. WeobservedthattheprotocolservicesusePython's Decimal tohelppreventunexpectedroundingissuesin off-chainmonetarycalculations.However,anincorrect variablewasusedinoneconsensus-impacting calculation(TOB-ELIXIR-4),indicatingthattheoff-chain arithmeticwouldbenefitfrommorethoroughtests. Moderate AuditingTheElixirsmartcontractsconsistentlyemiteventsthat includeenoughdataforeffectiveoff-chainmonitoring. EventandparameternamesprovidecontexT,although thesystemwouldbenefitfromadditionaldocumentation regardingtheimplicationsofeacheventaswellasan

incidentresponseplan. Theoff-chaincomponentsprintsufficientlogsfor monitoringtheinternalstate. Satisfactory Authentication/ AccessControls TheCorecontractmanagesgranularaccessrolesthat followtheprincipleofleastprivilege.Wedidnotidentify anymissingormisconfiguredaccesscontrols,althougha two-stepprocessforownershiptransferswouldhelp preventirrevocablemistakes(TOB-ELIXIR-15). Multipleissueswereidentifiedinoff-chainauthentication code.Forexample,the protocol-api authservicedoes notrevokeaccesswhen,forexample,avalidator's delegationsdropoutofthetop100ortheirIPaddress Weak hasheye 15ElixirProtocolSecurityAssessment PUBLIC

changes(TOB-ELIXIR-9). Complexity Management Smartcontractsandtheirmethodshavewell-defined responsibilitiesthatrelyonclearandconsistentnaming conventions.Weidentifiedfewinstancesofduplicate codeorfunctionswithhighcyclomaticcomplexity. EachPythonserviceadherestoapredictableand well-organizedstructure,aidingreviewofthecodebase. Satisfactory ConfigurationExampleenvironmentvariablevaluesclarifydeveloper intentandaidedourreview.However,weidentified someinstancesoferror-proneconfigurations,suchas theRedisactivation;(TOB-ELIXIR-5). Moderate Cryptography andKey Management Well-establishedlibrariesareusedtoperformsigning operationsandtointeractwithothercryptographic primitives.However,privatekeyspassthrough environmentvariablesduringstartup,increasingtherisk ofkeyexposure(TOB-ELIXIR-3).Weidentifiedaplace wherepartsofthepayloadarenotauthenticated (TOB-ELIXIR-16). Moderate DataHandlingSomesigningoperationshappenwithoutsufficient payloadvalidation(TOB-ELIXIR-6).Thereisnoclearly defineddatavalidationlayerforuntrusteduserinputin theAPI,whichledtoTOB-ELIXIR-7andTOB-ELIXIR-17. Weak DecentralizationThesmartcontractsdependonoff-chainservicesto function,onecomponentofwhichisacentralized messagedeliveryhub.Allsystemlogic,includingthe managementofuserELXtokens,isupgradablebya singleaccountwithoutgivingusersthechancetooptout. Weak DocumentationSmartcontractmethodsfeatureNatSpeccomments,and Pythonfunctionsaredescribedwithdocstrings.The systemarchitecturediagramprovidedcontextthataided ourreview.However,verylittlehigh-leveldocumentation wasprovided. Moderate Low-Level Manipulation ThesmartcontractsdonotrelyonanyEVMassembly codenoronanylow-levelcalls,apartfromthose includedinwellestablishedlibraries. Satisfactory hasheye 16ElixirProtocolSecurityAssessment PUBLIC

MaintenanceThecodeisorganizedintologicalmodules,makingit relativelystraightforwardtomaintain.However,outdated Pythondependencies(TOB-ELIXIR-1)indicatethelackofa processforupdatingdependenciesinatimelymanner; thesystemcouldbenefitfromtheuseoftoolssuchas DependabotinCItoautomaticallykeepdependenciesup todateintherepository. Moderate MemorySafety andError Handling TheprotocolservicesarewritteninPython,a memory-safelanguage,eliminatingthepossibilityof low-levelmemoryproblems.Errorhandlingisgenerally performedappropriately. Satisfactory Testingand Verification BothSolidityandPythonportionsofthecodebase featureunittests.However,mutationtestinguncovered someimportantgapsinSolidititytestcoverage,andsome oftheissuesweidentifiedcouldhavebeenfoundearlier withmorethoroughtests(TOB-ELIXIR-4). Moderate Transaction Ordering Weidentifiedissuesinthesmartcontractsthateither arisefrom,oraremademoresevereduето, transaction-orderingrisks.Thesystemwouldbenefit fromfurtherinvestigationandmorerigorous specificationoftimingrisks. Moderate hasheye 17ElixirProtocolSecurityAssessment PUBLIC

SummaryofFindings Thetablebelowsummarizesthefindingsofthereview,includingtypeandseveritydetailsIDTitleTypeSeverity 1UseofoutdateddependenciesPatchingInformational 2UseofHTTPrequestswithouttimeoutDenialofServiceInformational 3PrivatekeysstoredinenvironmentvariablesDataExposureHigh 4MajorityproposalgroupwillalwayssatisfyminimumsizerequirementDataValidationHigh 5AuthenticationatriskofreplayattacksifmisconfiguredConfigurationHigh 6StrategyexecutordoesnotvalidatepayloadtosignDataValidationHigh 7MissingIPaddressvalidationallowsbypassingRedpandaACLDataValidationMedium 8UseofassertstatementinproductioncodeDataValidationUndetermined 9RedpandaaccountsandassociatedpermissionsareneverrevokedAccessControlsUndetermined 10DelegatorscanredelegatestakestojailedelegateeDataValidationMedium 11AttackerscancauseslashingtobecomeeconomicallyinfeasibleDenialofServiceLow 12DelegatorscanimmediatelyundelegatebeforetheirdelegateeisjailedTimingHigh hasheye 18ElixirProtocolSecurityAssessment PUBLIC

13MinorityvalidatorsmayparticipateinconsensusprocessSessionManagementHigh 14AninfluxofnewstrategyexecutorsmayhaltconsensusDenialofServiceMedium 15Lackoftwo-stepprocessforownershiptransfersDataValidationInformational 16ResponsepayloadtoauthenticationchallengeisnotsignedCryptographyInformational 17APIdoesnotvalidatedisplay_nameandapp_versionDataValidationUndetermined 18Allon-chaineventsreplayeduponstartupDenialofServiceMedium 19RedpandaexposedtotheInternetConfigurationHigh

20APIhasadminaccesstoRedpandaConfigurationHigh 21Useofunpinnedthird-partyDockerimagesand actionsonworkflows ConfigurationLow 22Absenceofaccesscontrolsonpoolcreation function AccessControlsInformational hasheye 19ElixirProtocolSecurityAssessment PUBLIC

DetailedFindings 1.Useofoutdateddependencies Severity:InformationalDifficulty:Undetermined Type:PatchingFindingID:TOB-ELIXIR-1 Target:Multiple pyproject.toml , poetry.lock ,Dockerfiles Description Weused pipaudit todetecttheuseofoutdateddependenciesinthePythoncodebases, whichidentifiedanumberofvulnerablepackagesreferencedbythe pyproject.toml and poetry.lock files. Thefollowingisalistofthevulnerabledependenciesusedinthecodebase,andknown vulnerabilitiesthataffecttheversionsinuse: • certifi (GHSA-248v-346w-9cwc) • pysha3 (GHSA-6w4m-2xhg-2658) • requests (GHSA-9wx4-h78v-vm56) • urllib3 (GHSA-34jh-p97f-mpxf) Inmanycases,theuseofavulnerabledependencydoesnotnecessarilymeanthe applicationisvulnerable.Vulnerablemethodsfromsuchpackagesneedtobecalledwithin aparticular(exploitable)context.Todeterminewhethertheoff-chainapplicationsare vulnerabletotheseissues,eachissuewillhavetobemanuallytriaged.Theseverityis markedinformationalasuponpreliminaryinspection,theseissuesdonotappearto impactthecodebasedirectly. Moreover,theservicesuseanoutdatedversionofPython(3.10.12),whichwasreleasedon June6,2023.Anewerversion(3.10.14),releasedonMarch19,2024,isavailable; additionally,version3.12.4,releasedonJune6,2024,canbeusedifupgradingtotheminor versionisfeasible. Recommendations Shortterm,updatesystemdependenciestotheirlatestversionswhereverpossible.Use toolssuchas pipaudit toconfirmthatnovulnerabledependenciesremain. Longterm,implementthesechecksaspartoftheCI/CDpipelineofapplication development.IntegrateanautomatedsolutionsuchasDependabotintoyourdevelopment hasheye 20ElixirProtocolSecurityAssessment PUBLIC

processtoassistinpromptlydetectingandupdatingdependencieswithknownsecurity problems. hasheye 21ElixirProtocolSecurityAssessment PUBLIC

2.UseofHTTPrequestswithouttimeout Severity:InformationalDifficulty:High Type:DenialofServiceFindingID:TOB-ELIXIR-2 Target: elixir-protocol and elixir-protocol-api Pythonapplications Description TheElixiroff-chaincodeusesthePython requests librarytosendHTTPrequests.By default,requestsdonottimeoutunlessthe timeout parameterisexplicitlypassedtothe methodforarequest.Thisbehaviormaycausetheprogramtohangindefinitelywhenthe requestedserverissloworunresponsive.Theprogramssendrequestswithoutatimeout inthefollowinglocations: • TocreateanewuserinRedpanda: elixir-protocol-api/app/api/services/auth.py#L103 • Toresetanexistinguser’spassword: elixir-protocol-api/app/api/services/auth.py#L111 • TocancelallordersinVertex: elixir-protocol/services/failsafe_exchange_processor/failsafe_exc hange_processor/vertex/vertex_failsafe.py#L98 • TofetchthepoolconfigurationfromIPFS: elixir-protocol/services/onchain_pool_config_feed/onchain_pool_co nfig_feed/listeners/contract.py#L59 • TocreatenewordersinVertex: elixir-protocol/services/order_reconciler/order_reconciler/exchan ges/vertex/vertex_reconciler.py#L315 • TocancelordersinVertex: elixir-protocol/services/order_reconciler/order_reconciler/exchan ges/vertex/vertex_reconciler.py#L368 • Torequestanauthenticationchallengeasastrategyexecutor: elixir-protocol/services/strategy_executor/strategy_executor/elix ir_api.py#L22 • Tosubmitaresponsetoanauthenticationchallengeasastrategyexecutor: elixir-protocol/services/strategy_executor/strategy_executor/elix ir_api.py#L55 hasheye 22ElixirProtocolSecurityAssessment PUBLIC

Recommendations Shortterm,passanexplicit timeout parametertoall requests methods. Longterm,integratestaticanalysistoolssuchasBanditintoyoursoftwaredevelopment lifecycleandCI/CDprocesses.Theycandetectissuessuchasthisoneearlyoninthe developmentprocess. hasheye 23ElixirProtocolSecurityAssessment PUBLIC

3.Privatekeysstoredinenvironmentvariables Severity:HighDifficulty:High Type:DataExposureFindingID:TOB-ELIXIR-3 Target:Off-chainservicessigningkeys Description Elixir’soff-chainservicesareconfiguredviaenvironmentvariablesthatincludesensitive data,suchasprivatekeys,forsigning.Environmentvariablesarenotsuitableforstoring sensitivedata,astheymayleakviamultiplechannelssuchascrashreports.Examplesof thisconfigurationincludethe CONSENSUS_PROCESSOR_PRIVATE_KEY , STRATEGY_EXECUTOR_PRIVATE_KEY ,and FEED_AGGREGATOR_PRIVATE_KEY environment variables,whichareusedtosigncriticaldata. ExploitScenario Thefeedaggregatorservicecrashes,andthecrashreportcontaining FEED_AGGREGATOR_PRIVATE_KEY keymaterialisexportedtoathird-partyanalytics service. Recommendations Shortterm,resignfromusingenvironmentvariablesforconfiguringkeymaterial.Instead, fetchthekeymaterialonservicestartupfromadedicatedsecretstorageservice.Thiswill mitigatetheissueswithleakyenvironmentvariables. Longterm,useadedicatedserviceforsigninginsteadofstoringkeymaterialinindividual

services.Thiswillprotectthekeymaterialfromleakingviaotherchannelssuchascode executioninsidetheservices.ExamplesofmanagedsigningservicesincludeGoogleCloud KeyManagementServiceorAWSCloudHSM. hasheye 24ElixirProtocolSecurityAssessment PUBLIC

4.Majorityproposalgroupwillalwayssatisfyminimumsizerequirement Severity:HighDifficulty:High Type:DataValidationFindingID:TOB-ELIXIR-4 Target: elixir-protocol/services/consensus_processor/consensus_processor/con sensus_builder.py Description Theconsensusbuildercontainsachecktoensurethatthemajorityproposalgroupislarge enoughtoformconsensus.However,thecheckperformedisincorrectandwillneverfail.

```
#determineifenoughthemajorityproposalgroupisbigenoughtoformconsensus
consensus_proposal_group=majority_proposal_groups[0]
proposal_count=len(consensus_proposal_group.proofs)
minimum_requirement=math.ceil(proposal_count*self.min_consensus_threshold)
ifproposal_count<minimum_requirement: self.logger.info(
"Needtowaitformoreproposals,majorityproposalgrouponlyhas {proposal_count}proposals,
{minimum_requirement}proposalsarerequired", data_frame_id=data_frame_id, ) returnNone
```

Figure4.1:Thechecktoensurethatthemajorityproposalislargeenoughtoformconsensus (elixir-protocol/services/consensus_processor/consensus_processor/consens us_builder.py#L403-L412) Thischeckcomparestheproposalcountwiththeminimumrequirement,whichis computedasapercentageoftheproposalcount.Theproposalcountwillthereforenever belessthantheminimumrequirement. ExploitScenario Anattacker,whocontrolsasmallnumberofvalidatorsandiscapableofconfusingother validatorstoproduceinvalidproposals,obtainsasmallmajorityinthesystem.Thecheck toensurethatthemajorityislargeenoughdoesnottriggeradequately,andtheattacker’s proposalisaccepted. Recommendations Shortterm,correctthechecksothatitcorrectlycomputestheminimumrequirement, possiblyasapercentageofthetotalproposals. hasheye 25ElixirProtocolSecurityAssessment PUBLIC

Longterm,implementunittestsforimportantfunctionalitytoensurethatitbehavesas intended. hasheye 26ElixirProtocolSecurityAssessment PUBLIC

5.Authenticationatriskofreplayattacksifmisconfigured Severity:HighDifficulty:High Type:ConfigurationFindingID:TOB-ELIXIR-5 Target: elixir-protocol-api authentication Description The elixir-protocol-api authenticationisvulnerabletoreplayattacksiftheserviceis everrunwith config.redis_enabled setto False .Theimplementationofthe connect and verify endpointsenablesrunninginthisconfigurationwithoutreportinganyerror (figures5.1and5.2).Insuchacase,the nonce issetto None ,and connect returnsthe message“ElixirProtocolVerificationMessage.None”tosign.Thesamehappensin verify , whichwillvalidatemessageswith None asa nonce .

```
defconnect(self,address:str):
"""Createamessageforthevalidatortosign.""" nonce=None key=f"validator-nonce-{address}"
#checktoseeifwehaveanonceforthisvalidator. ifself.config.redis_enabled:
redis=self.redis_service.get_redis() nonce=redis.get(key) ifnonceisNone: nonce=uuid.uuid4()
redis.set(key,nonce,ex=None) return{"message":f"{SIGNED_MESSAGE}{nonce}","nonce":nonce,"address":
address}
```

Figure5.1:Thevulnerable connect endpointfunction (elixir-protocol-api/app/api/services/auth.py#L45-L59)

```
nonce=None redis=self.redis_service.get_redis()
#searchforsavednoncevalue ifself.config.redis_enabled: nonce=redis.get(f"validator-nonce-
{address}") ifnotnonce: raiseHTTPException(status_code=401,detail="INVALID_NONCE")
```

hasheye 27ElixirProtocolSecurityAssessment PUBLIC

```
#recovertheaddress message=encode_defunct(text=f"{SIGNED_MESSAGE}{nonce}")
recovered_address=self.web3.w3.eth.account.recover_message(message,
signature=signature.replace('"',""))
```

Figure5.2:Thevulnerable verify endpointfunction (elixir-protocol-api/app/api/services/auth.py#L167-L179) ExploitScenario Anattackercapturesasigned“ElixirProtocolVerificationMessage.None”messageand replaysitwhiletheAPIserviceismisconfiguredwith config.redis_enabled setto False .TheattackerthengainsaccesstotheRedpandaeventbus. Recommendations Shortterm,reject connect and verify requestswith500or503statuscodeifRedisis disabledinaproductionenvironment.DisablingRedisshouldnotmakethesystem insecure. Longterm,explicitlymarkinsecureconfigurationoptionswithunsafewordingandmakeit impossibletoturnthemonoutsideofthedevelopmentenvironment. hasheye 28ElixirProtocolSecurityAssessment PUBLIC

6.Strategyexecutordoesnotvalidatepayloadtosign Severity:HighDifficulty:High Type:DataValidationFindingID:TOB-ELIXIR-6 Target: elixir-protocol/services/strategy_executor/strategy_executor/elixir_ api.py Description ThestrategyexecutorservicesignstheauthenticationmessagefromtheAPIwithout validatingitsstructure(figure6.1).Theservercanabusethisfunctionalitytosignarbitrary EIP-191 personal_sign messagesandusethemasiftheywereoriginallysignedbythe strategyexecutor.

authentication_message=authentication["message"]
validator_address=get_address_from_key(private_key)
self.logger.info("Sendingauthorizationrequest",address=validator_address)
#sendsignedmessagebacktoapiforverification message=encode_defunct(text=str(authentication_message))
signature=Web3().eth.account.sign_message(message,private_key=private_key)
Figure6.1:Strategyexecutorsigningdatawithoutvalidatingitsstructure (elixir-protocol/services/strategy_executor/strategy_executor/elixir_api. py#L47-L53) ExploitScenario AnattackerwhocontrolstheAPIreplieswithanauthenticationmessagethatisamalicious OrderProposalDetail payload.Thepayloadissignedbythestrategyexecutorand returnedtotheattacker.Theattackercansubmitafraudulentorderproposalonbehalfof theexecutorbecause,duringtheregularoperation,thestrategyexecutorsignsthis structurewiththesamekey. Recommendations Shortterm,validatethestructureoftheauthenticationmessagereturnedbytheAPI server.Makesuretovalidatethelengthandstructureofthenoncetopreventinjection attacks. Longterm,ensurethatthepayloadstructureisalwaysvalidatedbeforeeachsigning operation. hasheye 29ElixirProtocolSecurityAssessment PUBLIC

7.MissingIPaddressvalidationallowsbypassingRedpandaACL Severity:MediumDifficulty:Low Type:DataValidationFindingID:TOB-ELIXIR-7 Target: elixir-protocol-api/app/api/services/auth.py Description TheIPaddressusedtocreateRedpandaACLsisnotvalidated,whichallowsbypassingthe hostrestrictionfromACLs(figure7.1).BecausetheIPaddresscanbeanarbitrarystring,it ispossibletosendanallhostswildcard(*)insteadofaconcreteIPaddress.
defcreate_acls(self,username:str,ip_address:str): """CreateACLsinredpandaforuser."""
self.logger.info("CreatingACLs")
admin_client=KafkaAdminClient(bootstrap_servers=self.config.event_bus_brokers) read_acl=ACL(
principal=f"User:{username}", host=ip_address, operation=ACLOperation.READ,
permission_type=ACLPermissionType.ALLOW,
resource_pattern=ResourcePattern(ResourceType.TOPIC,DATA_FRAME_TOPICS),) write_acl=ACL(
principal=f"User:{username}", host=ip_address, operation=ACLOperation.WRITE,
permission_type=ACLPermissionType.ALLOW,
resource_pattern=ResourcePattern(ResourceType.TOPIC,ORDER_PROPOSAL_TOPICS),)
Figure7.1:UnvalidatedIPaddressendsupstraightinACLs (elixir-protocol-api/app/api/services/auth.py#L125-L144) ExploitScenario Amaliciousstrategyexecutorsendsa * insteadofaconcreteIPaddresstoverifyan endpoint.TheyusetheRedpandacredentialstoexecuteadistributeddenial-of-service attack. Recommendations Shortterm,requiretheIPaddresssentbystrategyexecutorstobeaconcretevalue,or taketheIPaddressfromtheconnectioninsteadoftheuserhavingtoprovideit. hasheye 30ElixirProtocolSecurityAssessment PUBLIC

8.Useofassertstatementinproductioncode Severity:UndeterminedDifficulty:High Type:DataValidationFindingID:TOB-ELIXIR-8 Target: elixir-protocol/services/strategy_executor/strategy_executor/glt_str ategy.py , elixir-protocol/shared/shared/event_scanner/event_scanner.py Description Whenoptimizationsarerequestedwiththe -O flag,assertstatementsareremovedfrom theprogram.Thefollowingfunctionsuseassertstatementsthatwillbeskippedif optimizationsareenabled. • GltStrategy.get_balance • GltStrategy.get_price • GltStrategy.get_metrics • GltStrategy.apply_order_level • EventScanner.scan ExploitScenario Thestrategyexecutorisrunwithoptimizationsenabled,andthe apply_order_level functionoperatesonaninvalidproposalwithamismatchednumberofbuysandsells, leadingtoundefinedbehavior. Recommendations Shortterm,changetheassertstatementstostatementsthatexplicitlyraiseexceptions. Thiswillremovetheriskthatthevalidationlayerwillbeoptimizedout. Longterm,integratestaticanalysistoolssuchasBanditintoyoursoftwaredevelopment lifecycleandCI/CDprocesses.Theycandetectissuessuchasthisoneearlyoninthe developmentprocess. hasheye 31ElixirProtocolSecurityAssessment PUBLIC

9.Redpandaaccountsandassociatedpermissionsareneverrevoked Severity:UndeterminedDifficulty:High Type:AccessControlsFindingID:TOB-ELIXIR-9 Target: elixir-protocol-api/app/api/services/auth.py Description Aspartoftheauthenticationprocess,whenastrategyexecutorclientcallsthe /verify API endpointwithavalidrequestthatmeetsalltherequirementstoparticipateinthesystem, theback-endservicewillcreateorupdateanaccountintheRedpandamessagebrokerfor thestrategyexecutorclienttouse,alongwithapairofACLrulesthatallowconnectionsas thisusernamefromacertainIPaddress.However,thereisnomechanismtoexpireor disabletheseaccounts,soclientsthatstopparticipatingorarejailedcontinuetohave accesstotheeventbus.Additionally,anewpairofACLrulesarecreatedeachtimeauser connects,andpreviousACLrulesarenotclearedfromRedpanda.Asaresult,anaccount maybeaccessiblefrommultipleIPaddresseseveninabsenceofanissuelikeTOB-ELIXIR-7. ExploitScenario#1 AmaliciousstrategyexecutoroperatorrepeatedlylogsinwithmultipleconcreteIP addressestothe /verify

endpoint.AsACLsdonotgetcleared,theRedpandauserisnow accessiblefromalltheIPaddressesprovidedbythemaliciousoperator.Theythen distributethecredentialsobtainedonthelastloginoperationandexecuteadistributed denial-of-serviceattack. ExploitScenario#2 Astrategyexecutoroperatingwithaddress 0xA andatokendelegationfromaddress 0xB is compromisedandtheattackerextractstheRedpandacredentialsinuse.Theoperator containsthecompromisebyrotatingthestrategyexecutorkeys,whichwillnowusewallet 0xC ,andbymoving 0xB ’sdelegationtothenewaddress.Whilethepreviousaddressis nowunsuitabletologinthroughtheprotocolAPIbackend,asithasnotokensdelegated toit,theattackercanstillusetheRedpandacredentialstoobservemessagesorperforma denial-of-serviceattack. Recommendations Shortterm,implementcredentialrevocation.OldACLrulesforausershouldberevoked whenanewauthenticatedsessionisestablished.Thiswillgiveuserstheabilitytoremove oldentriesinthecaseofcompromise.Inaddition,accessshouldberevokedifusersare jailedortheirdelegationsdroptozero. hasheye 32ElixirProtocolSecurityAssessment PUBLIC

Longterm,reviewauthorizedpermissionsandthecontextsinwhichtheyarevalid.Itis equallyimportanttoensurethatauthorizationsarerevokedwhenvalidcontextsbecome invalid,asitiswhenvalidcontextsareoriginallyestablished. hasheye 33ElixirProtocolSecurityAssessment PUBLIC

10.Delegatorscanredelegatestakestojaileddelegatee Severity:MediumDifficulty:Low Type:DataValidationFindingID:TOB-ELIXIR-10 Target: elixir-protocol/contracts/src/StakeManager.sol Description Theinternal _updateDelegation helpermethoddoesnotpreventusersfromdelegating toavalidatorthatisjailed,allowinghonestuserstoaccidentallyloseaccesstotheirstake. The delegate functionisresponsibleforhandlingbothdelegationandredelegation actions.Duringredelegation,severalvalidationchecksareperformed:ensuringthatthe redelegationhasbeensignaledinadvance,confirmingthatthecurrentdelegateeofthe delegatorisnotjailed,andverifyingthedelegatorhasnotsignaledanunstake.However, thestatusofthenewdelegatee,towhomthedelegatorintendstomovetheirstakes,isnot checkediftheyarejailed.Thisallowsforredelegationtoajailedvalidator,leadingto potentiallossoffundsforthedelegator. ExploitScenario BobnoticesthatAlicerunsavalidatorwithagoodperformancehistory,butheisunaware thatAlicerecentlymisbehaved.BobsendsatransactiondelegatinghisstaketoAliceright afteranotherusersendsatransactionjailingAlice,andbothtransactionssucceed.Asa result,Bobinadvertentlylosesaccesstohisfunds. Recommendations Shortterm,addachecktothe _updateDelegation methodthatrevertsatransaction thatattemptstodelegatetoavalidatorwhohasbeenjailed. Longterm,strivetomakeitashardaspossibleforanhonestusertomakeacostly mistake.Payparticularattentiontoraceconditionsthatoccurduringcontractstate transitions. hasheye 34ElixirProtocolSecurityAssessment PUBLIC

11.Attackerscancauseslashingtobecomeeconomicallyinfeasible Severity:LowDifficulty:High Type:DenialofServiceFindingID:TOB-ELIXIR-11 Target: elixir-protocol/contracts/src/StakeManager.sol Description The slash functiontakesasingleaddressasaparameter,alongsidetheamounttobe slashed.Whenasignificantnumberofusersneedstobeslashed,theslashfunctionmust becalledeachaddressindividually.Thisapproachbecomesinfeasibleifthereisalarge numberofsmalldelegations. ///@noticeSlashesastaker ///@paramstakerStakertobeslashed ///@paramamountAmounttobeslashed functionslash(addressstaker,uint256amount)externalonlyCore{ //Reducesstakedbalance. stakedBalance[staker]-=amount; //Reduceddelegatedbalance. _moveDelegates(delegates[staker],address(0),amount); //Transfersthetokens. elixirToken.safeTransfer(msg.sender,amount); emitSlashed(staker,amount,stakedBalance[staker]); } Figure11.1:Theslashmethod(StakeManager.sol#L271-L285) Basedonthecurrentdesignoftheprotocol,whenavalidatorisjailed,alldelegatorswho stakedwiththatjailedvalidatorwillhavetheirstakeslockedandpotentiallyslashed. However,intheeventofslashing,eachaffecteddelegatorneedstobeslashedindividually. Thecostofperformingslashingontheentiresetofaffecteddelegatorsincreases proportionallywiththenumberofdelegatorsinvolved.Incaseswherethenumberof affecteddelegatorsissignificantlylarge,thehighcostmaydiscouragetheexecutionof slashing,allowingdelegatorstoevadetheintendedpenalty. ExploitScenario BobacquiresELXtokenswiththeintentofmisbehaving.Togrieftheprotocolbymakingit lesscosteffectiveforhimtobeslashed,hedistributessmallamountsofhistokensamong alargenumberofaccountsanddelegatesthemalltohimself.AfterBobisjailedforacting maliciously,thecostofrecoveringELXfromhisdelegatorsisprohibitivelyexpensive. hasheye 35ElixirProtocolSecurityAssessment PUBLIC

Recommendations Shortterm,considerimplementinganadditionalbatchslashmethodinthe StakeManager contractthatacceptsanarrayofaddressesandslasheseachdowntoazerobalance.Some arithmeticandconditionallogiccanbeskipped,makingthisacheaperandeasierwayto recoverfundsfromalargenumberofmisbehavingaccounts. Longterm,keepinmindthatadelegateewithasmallnumberoflargedelegatorsmay haveanequalweightasadelegateewithalargenumberofsmalldelegators.Consider bothsituationsandwaysanattackermaytakeadvantageofdifferencessuchasgas economics. hasheye 36ElixirProtocolSecurityAssessment PUBLIC

12.Delegatorscanimmediatelyundelegatebeforetheirdelegateeisjailed Severity:HighDifficulty:Low Type:TimingFindingID:TOB-ELIXIR-12 Target: elixir-protocol/contracts/src/StakeManager.sol Description Thereisnopenaltyforpreemptivelysignalingredelegationimmediatelyafterinitial delegation.Doingso(andwaitingthroughthecooldown)wouldgivedelegatestheabilityto front-runfuturejailtransactionsandavoidhavingtheirfundslocked,effectivelybypassing thedelaythatsignalingissupposedtoimpose. Aspartofthefront-runningprotectionmechanismdesignedtopreventdelegatorsfrom unstakingorredelegatingjustbeforetheirdelegateeisjailed,delegatorsarerequiredto signalanundelegateandwaitfortheexpirationofawaitingperiodbeforeproceedingwith theundelegation.However,the signalUndelegate functioncanbeinvokedatthestartof thedelegationperiod.Oncethewaitingperiodhaspassed,theundelegation/redelegation requirementismet,allowingthedelegatortomaintainthisstateandimmediately undelegateorredelegateatanytime.Thisisparticularlyproblematicifthedelegateeis abouttobejailed,asthedelegateejailtransactioncanbefront-runwithanundelegateor redelegatetransactiontoavoidthepenalty. ExploitScenario AlicedelegatesherstakewithBobthedelegatee,immediatelyafterthedelegation,she signalsundelegatewhilemaintainingherdelegationwithBobevenwhentheundelegation waitingperiodhaspassed.Bobisabouttobejailed,shenoticesajailtransactionforBobin thempoolandfront-runsitwithanundelegatetransactionwhichgetsexecutedfirst allowinghertoeffectivelyevadethejail Recommendations Shortterm,delegatorsthathavesignaledredelegateshouldbeexcludedfromavalidator’s totaldelegations. Longterm,keepinmindthattimestampsontheblockchainareerrorproneandafrequent sourceoferrors.Reviewalltimestampsusedbythesystemand,foreach,considerwhat wouldhappenimmediatelybeforeandafterimportantthresholdsaswellasatthe extremes.Thiswillfacilitateareviewofthecodebaseandhelppreventsimilarproblems. hasheye 37ElixirProtocolSecurityAssessment PUBLIC

13.Minorityvalidatorsmayparticipateinconsensusprocess Severity:HighDifficulty:Medium Type:SessionManagementFindingID:TOB-ELIXIR-13 Target: elixir-protocol/services/consensus_processor/consensus_processor/con sensus_builder.py Description Theconsensusbuilderreceivesandconsidersanyproposalsfromactivevalidatorstowards itsgoalofachievingconsensus.Activevalidatorsarethosewithanon-zerodelegationand whicharenotjailed.Consideringthataccesstovalidatorsisnotrevokediftheirdelegated tokenamountbecomessmall(seeTOB-ELIXIR-9),thiscouldallowoneormanyminority strategyexecutors(i.e.,thosewithasmalldelegation,andthatshouldnotbepartofthe “core”set)toparticipateintheconsensusprocess.Amaliciousactormaytakeadvantageof thisfacttogainamajorityoftheconsensusvote. ExploitScenario Assumingthatthetop99validatorshaveover1,000tokensdelegatedeach,anattacker obtains1,001tokens.Theattackerdevelopsamaliciousstrategyexecutorsoftwarethatwill forthemostpartbehaveidenticallytotheofficialsoftware;however,whenitreceivesa specialsignal,itwillsubmitamaliciousproposal. Theattackerthendelegatestheirtokenstotheaddress 0xA ,andrunsamaliciousstrategy executorwiththisaddress.Oncetheexecutorisonline,theattackerredelegatesallbutone centofthetokentoanewaddress, 0xB ,andrepeatstheprocess.Eachtime,whenthe freshly-delegated-tovalidatorattemptstologintothesystem,thisvalidatorwillbe consideredpartofthe“core”listandbeallowedtoconnecttoRedpanda,astheir delegationwillbeoneofthetop100(CORE_VALIDATOR_SET_SIZE)largestbyamount delegated.Thisprocessisrepeated200times,untiltheattackerisoperatingamajorityof theactivevalidatorsthatcanparticipateinconsensus. Theattackercanthenchoosetooperatetheirstrategyexecutorsbenevolently,andcollect anoutsizedshareofthesystemrewards.However,theattackercanalsoopttosignalto theirvalidatorswhenthemarketconditionsarebeneficial,andalloftheirexecutorswill thensubmitacoordinated,maliciousproposal,whichbecomesthemajorityproposaland gainsconsensus.Thesystemthenexecutesthemaliciousproposal,andpotentiallyjails goodvalidators,furtherstrengtheningtheattacker’sposition. hasheye 38ElixirProtocolSecurityAssessment PUBLIC

Recommendations Shortterm,implementamechanismtodisconnectandrevokeRedpandaaccessfrom strategyexecutorsthatshouldnotbepartofthecoreset.Enforcesomesortofminimum delegationvaluetobeabletoparticipateinconsensus. Longterm,runathreatmodelingexercisecoveringtheinteractionofuserswith permissionedandpermissionlesscomponentswithinthesystem.Thisexerciseshould identifyasystem'sspecificrisksandtheactorsthatcouldtakeadvantageofthem,both outside(e.g.,validators,third-partyproviders)andfromwithin(e.g.,contractoperators). hasheye 39ElixirProtocolSecurityAssessment PUBLIC

14.Aninfluxofnewstrategyexecutorsmayhaltconsensus Severity:MediumDifficulty:Low Type:DenialofServiceFindingID:TOB-ELIXIR-14 Target: elixir-protocol-api/app/api/services/auth.py , elixir-protocol/services/consensus_processor/consensus_processor/con sensus_builder.py Description Theconsensusbuilderrequiresaminimumnumberofproposalstoachieveconsensus,as oneofitsmanychecks.Thisminimumrequirementiscomputedasapercentageofactive (i.e.withanon-zerodelegationandnotjailed)validators,asshowninfigure14.1. defget_active_validators(self,data_frame:DataFrame): returndata_frame.data_frame_detail.active_validators.validator_addresses defget_min_required_proposals(self,data_frame:DataFrame): active_validators=self.get_active_validators(data_frame) returnmath.ceil(len(active_validators)*self.min_validators_threshold) defhas_minimum_proposals(self,data_frame:DataFrame): total_proposals=self.get_proposal_count(data_frame) min_required_proposals=self.get_min_required_proposals(data_frame) returntotal_proposals ⩾ min_required_proposals Figure14.1:Thechecktoensurethattherearеenoughproposals (elixir-protocol/services/consensus_processor/consensus_processor/consens us_builder.py#317-327) However,theauthenticationendpointverification(/verify APIroute)willallowonlya fixednumber(CORE_VALIDATOR_SET_SIZE)ofvalidatorstologinandobtainRedpanda access;thisvalueiscurrentlysetto100.Thismeansthat,withalargeenoughnumberof validators,consensusmaybecomeunachievable,as100validatorsmaynotbeenoughto complywiththeminimumnumberofproposalsrequiredforconsensus. #determineifthevalidatorisinthecorevalidatorset validators=validator_service.get_validators(offset=0,limit=CORE_VALIDATOR_SET_SIZE,order_by="total_delegated", order_dir="desc") matches=list(filter(lambdav:v.address==existing.address,validators)) ifnotmatches: hasheye 40ElixirProtocolSecurityAssessment PUBLIC

#createauthenticationevent self.create_authentication_event(existing.address,False) raiseHTTPException(status_code=401,detail="EXCLUDED_ADDRESS") Figure14.2:The /verify APIendpointwillnotletallvalidatorsin (elixir-protocol-api/app/api/services/auth.py#80-89) ExploitScenario Anattackersplitstheirtokensamong202addressesanddelegatesthemto202different validators,sothattheminimumproposalsrequiredtoachieveconsensusincreasesby101 (50%of202).Asaresult,thesystemishaltedandnofurtherconsensuscanbeachieved becauseonly100validatorsmayconnecttoRedpandaandtheconsensusbuildercannot receiveenoughproposalsineachround. Recommendations Shortterm,adjustthelogicsothattheminimumproposalsrequiredareafunctionofthe smallestamongtheamountofparticipatingvalidatorsorthecorevalidatorsetsize.Note thatdynamicallyadjustingthesizeofthecorevalidatorsetinrelationtothetotalnumber ofvalidatorsmaynotbeenough,asmaliciousvalidatorsmaypurposelydecidenotto participateinconsensus. Longterm,runathreatmodelingexercisecoveringtheinteractionofuserswith permissionedandpermissionlesscomponentswithinthesystem.Thisexerciseshould identifyasystem'sspecificrisksandtheactorsthatcouldtakeadvantageofthem,both outside(e.g.,validators,third-partyproviders)andfromwithin(e.g.contractoperators). hasheye 41ElixirProtocolSecurityAssessment PUBLIC

15.Lackoftwo-stepprocessforownershiptransfers Severity:InformationalDifficulty:High Type:DataValidationFindingID:TOB-ELIXIR-15 Target: elixir-protocol/contracts/src/* Description Whencalled,the transferOwnership functionimmediatelysetsthecontractownerto theprovidedaddress.Theuseofasinglesteptomakesuchacriticalchangeiserror-prone; ifthefunctioniscalledwitherroneousinput,theresultscouldbeirrevocableordifficultto recoverfrom. Theissueispresentinthefollowingcontracts: • Core • DisputeManager • ELX • Pool • PoolManager • StakeManager Therequirementforaseparateacceptancestepbeforeroletransferiscompletedwill guaranteethatthenewownercanproperlyexecutetransactionsonthecontractsitwillbe administering. ExploitScenario Aliceinvokes transferOwnership tochangethecontractownerbutaccidentallyenters thewrongaddress.Shepermanentlylosestheabilitytosetimportantsystemparameters andupgradethecontract. Recommendations Shortterm,implementatwo-stepprocessforallirrecoverablecriticaloperations.Consider usingthe Ownable2StepUpgradeable OpenZeppelindependencyinsteadof OwnableUpgradeable

forownershipmanagement. Longterm,identifyanddocumentallpossibleactionsthatcanbetakenbyprivileged accounts,alongwiththeirassociatedrisks.Thiswillfacilitatereviewsofthecodebaseand preventfuturemistakes. hasheye 42ElixirProtocolSecurityAssessment PUBLIC

16.Responsepayloadtoauthenticationchallengeisnotsigned Severity:InformationalDifficulty:High Type:CryptographyFindingID:TOB-ELIXIR-16 Target: elixir-protocol/protocol/services/strategy_executor/strategy_executo r/elixir_api.py , elixir-protocol-api/app/api/services/auth.py Description Duringtheauthenticationprocess,thestrategyexecutorsignsachallengemessagewitha nonceandreturnsittotheAPItoobtaincredentials,togetherwithotherinformationsuch asitsIPaddress,displayname,beneficiaryaddress,andapplicationversion.However, theseadditionaldetailsarenotcoveredbythesignature,sotheirauthenticitycouldbe compromised.Thisis,however,unlikely,astheexchangeoccursoveraTLSconnection. ExploitScenario Anattackeronthesamenetworkasthestrategyexecutorperformsa machine-in-the-middle(MitM)attacktointerceptandmodifythechallenge-response authenticationmessages.Theydosobytakingadvantageofacompromisedormalicious rootCAinstalledonthestrategyexecutormachine.Thestrategyexecutorrequestsa challengefromtheserver,signsit,andreturnsittogetherwiththeirIPaddress,display name,beneficiaryaddress,andapplicationversion.Theattackerchangesthebeneficiary addresstoadifferentoneundertheircontrolbeforepassingthemessageovertothe /verify endpoint.Theserveracceptsthechallenge,usesthemodifiedbeneficiary address,andpaysoutthevalidatorrewardstotheattacker. Recommendations Shortterm,includetheseextradetailsorahashofthemaspartofthesignedmessage,so thattheprotocolAPIcanverifythattheyhavenotbeentamperedwith.Considerpinning thecertificatesusedbytheprotocolAPIinthestrategyexecutortoensurethatthe communicationscannotbesenttoanunexpectedparty. hasheye 43ElixirProtocolSecurityAssessment PUBLIC

17.APIdoesnotvalidatedisplay_nameandapp_version Severity:UndeterminedDifficulty:High Type:DataValidationFindingID:TOB-ELIXIR-17 Target: elixir-protocol-api/app/api/services/auth.py Description Duringtheauthenticationprocess,theprotocolAPIserverreceivesa“displayname”string andtheapplicationversionstringprovidedbythestrategyexecutor.Thesestringsare arbitraryandtheyarenotvalidatedeitherinlengthorcontents.Anattackermaysend largeamountsofdatatocauseadenialofservice,orabusetheunsanitizedstoragefor maliciouspayloads. ExploitScenario Amaliciousstrategyexecutorsubmitsacross-sitescripting(XSS)payloadastheirdisplay name.Thatstringisthenrenderedunsafelyinafutureadministrativepaneldevelopedby Elixir,andmaliciouscodegetsexecutedinthatcontext. Recommendations Shortterm,ensurethatbothstringsconformtoanexpectedformatandmaximumlength, andsanitizetheircontentsbeforestoringthem. Longterm,validateandsanitizeanyuntrusted,user-providedinputthatisreceivedbythe system. hasheye 44ElixirProtocolSecurityAssessment PUBLIC

18.Allon-chaineventsreplayeduponstartup Severity:MediumDifficulty:High Type:DenialofServiceFindingID:TOB-ELIXIR-18 Target: feed_aggregator , message_recorder , metrics_recorder , strategy_metrics services Description The feed_aggregator , message_recorder , metrics_recorder ,and strategy_metrics servicesreplayonstartupalleventsfromthebeginningofthehistory (figure18.1).Thismakestheservicesvulnerabletodenialofserviceifthehistorytakesa longtimetoprocess.Inotherwords,theprogressinprocessingeventsisnotpersisted throughoutrestartsofaservice. onchain_feed_consumer=SharedQueueConsumer(brokers=config.event_bus_brokers, topics=config.event_bus_onchain_feed_topics, shared_data_queue=shared_data_queue, offset=OFFSET_MODE_EARLIEST,) Figure18.1:Theconsumerconfigurationresponsibleforreplayingallevents (elixir-protocol/services/feed_aggregator/feed_aggregator/__main__.py#L35 -L40) ExploitScenario Anattackerfindsawaytopersistalargeamountofeventsthatareprocessedonstartupin oneofthevulnerableservices.Theattackereitherfindsawaytocrashtheserviceorwaits fortheservicerestart.Theservicetakesalongtimetostartanditisnotservingitspurpose duringthattime. Recommendations Shortterm,updatetheservicestopersistthestatebuiltfromtheeventstream.Thiscan happeneveryevent,afterabatchofevents,orperiodically,dependingontheperformance requirements.Itisimportanttopersisttheeventstreamoffsetatomicallywiththestate builtontheeventsuptotheoffset.Ifthecachedstatedataschemachanges,itcanbe eithermigratedorpurged(sincetheeventstreamistheauthoritativesource).Ifitis purged,thestatehastoberebuilt;however,sincethisisaone-timeevent,itshouldnot significantlyincreasetheriskofadenial-of-serviceattack. hasheye 45ElixirProtocolSecurityAssessment PUBLIC

Longterm,addteststhatcheckdataintegritybetweentheeventhistoryandthecached stateandensurethatservicesarestartinginatimelymannereveninthefaceofmassive amountsofdata. hasheye 46ElixirProtocolSecurityAssessment PUBLIC

19.RedpandaexposedtotheInternet Severity:HighDifficulty:High Type:ConfigurationFindingID:TOB-ELIXIR-19 Target: Redpanda Description TheconsequenceofElixir'soff-chainsystemarchitectureisthattheRedpandabrokeris exposedtotheinternet,asthestrategyexecutorsconnectdirectlytothebroker.This makesRedpandaeasilyaccessibletoattackers,astheycandirectlytrytoexploittheservice overthenetwork.Theconsequencesofthisdesigndecisionalsomanifestinfindings TOB-ELIXIR-9andTOB-ELIXIR-20. ExploitScenario Aremotelyexploitablevulnerability,suchasCVE-2023-50976,isdiscoveredinRedpanda. BecauseRedpandaisaccessibleoverthenetworktoanyone,attackerseasilyexploitthis vulnerability,potentiallygainingwriteaccessorperformingadenial-of-serviceattack. Recommendations Shortterm,hideRedpandainstancessotheyareaccessibleonlyontheinternalnetworkto therelevantservices.UseACLstolimitaccesstotheminimumrequiredbyeachservice. AddfunctionalitytotheAPIservicetostreamdataframestoandreceiveorderproposals fromstrategyexecutors. Longterm,alwayslimitpublicnetworkaccessasmuchaspossibleandexposeonlythe necessaryAPIs. hasheye 47ElixirProtocolSecurityAssessment PUBLIC

20.APIhasadminaccesstoRedpanda Severity:HighDifficulty:High Type:ConfigurationFindingID:TOB-ELIXIR-20 Target:APIservice,Redpanda Description TheAPIservicehasadminaccesstoRedpandatoconfigureusers(figure20.1)andACLs (figure20.2).Havingsuchpowerfulcapabilityinaserviceexposedtotheinternetputs Redpandaatahighriskofexploitation. defcreate_user(self,address:str): """Createanewuser.""" username=f"user_{address}" password=secrets.token_urlsafe(32) #createuser self.logger.info("Creatinguser") create_response=requests.post(f" {self.config.admin_event_bus_brokers}/v1/security/users", json= {"username":username,"password":password,"algorithm": "SCRAM-SHA-256"},) #checkresponsecode ifcreate_response.status_code==500and"Useralreadyexists"in create_response.text: #updateuserinformation update_response=requests.put(f" {self.config.admin_event_bus_brokers}/v1/security/users/{username}", json= {"password":password,"algorithm":"SCRAM-SHA-256"},) Figure20.1:APIusesadminendpointstoconfigureRedpandausers (elixir-protocol-api/app/api/services/auth.py#L96-L123) defcreate_acls(self,username:str,ip_address:str): """CreateACLsinredpandaforuser.""" self.logger.info("CreatingACLs") admin_client=KafkaAdminClient(bootstrap_servers=self.config.event_bus_brokers) read_acl=ACL(principal=f"User:{username}", host=ip_address, operation=ACLOperation.READ, hasheye 48ElixirProtocolSecurityAssessment PUBLIC

permission_type=ACLPermissionType.ALLOW, resource_pattern=ResourcePattern(ResourceType.TOPIC,DATA_FRAME_TOPICS),) write_acl=ACL(principal=f"User:{username}", host=ip_address, operation=ACLOperation.WRITE, permission_type=ACLPermissionType.ALLOW, resource_pattern=ResourcePattern(ResourceType.TOPIC,ORDER_PROPOSAL_TOPICS),) try: admin_client.create_acls([read_acl,write_acl]) exceptExceptionase: self.logger.error("ErrorcreatingACLs",exception=e) raiseHTTPException(status_code=500,detail="BROKER_ERROR") Figure20.1:APIusesadminendpointstoconfigureACLs (elixir-protocol-api/app/api/services/auth.py#L125-L150) ExploitScenario AnattackerfindsawaytoexecutecodeinthecontextofanAPIserviceandusesitto reconfigureRedpandatobeaccessibleforanywrites. Recommendations Shortterm,hideRedpandainsidetheinternalnetwork,asdetailedintheshort-term recommendationforTOB-ELIXIR-20.Thiswillremovetheneedfordynamicconfigurationof RedpandausersandACLsfromtheAPI,thusremovingtheneedforhavingadminaccess. Longterm,avoidgivingthepowerofadministrativetaskstoservicesexposedtothe internet. hasheye 49ElixirProtocolSecurityAssessment PUBLIC

21.Useofunpinnedthird-partyDockerimagesandactionsonworkflows Severity:LowDifficulty:High Type:ConfigurationFindingID:TOB-ELIXIR-21 Target: elixir-protocol/.github/workflows/{abis.yaml,contracts.yml,strategy_ executor.yml} ,multipleDockerfiles Description Severalworkflowsintherepositorydirectlyusethird-partyactionssuchas stefanzweifel/git-auto-commit-action@v5 , foundry-rs/foundry-toolchain@v1 , docker/setup-qemu-action@v2 , docker/setup-buildx-action@v2 , docker/login-action@v2 , docker/build-push-action@v3 ,and juliangruber/read-file-action@v1 .Someof theseworkflowshaveprivilegedaccesstosecretssuchasDockerHubtokens,orwrite accesstotherepository. - uses:stefanzweifel/git-auto-commit-action@v5 with: commit_message: ⍰ autoupdatingABIs Figure21.1:Anexampleworkflowusingathird-partyactionreferencedbyitstag (elixir-protocol/.github/workflows/abis.yaml#57-59) Gittagsaremalleable.Thismeansthatwhile,forexample, juliangruber/read-file-action ispinnedto v1 ,theupstreammaysilentlychange thereferencepointedtoby v1 .Thiscanincludemaliciousre-tags,whichmaycauseElixir's

workflowtosuddenlystartexecutingmaliciouscode. GitHub’ssecurityhardeningguidelinesforthird-partyactionsencouragedeveloperstopin third-partyactionstoafull-lengthcommithash.Generallyexcludedfromthisare“official” actionsunderthe actions organization;however,theseotheractionsarenotdeveloped byGitHub. SeveralDockerfilesintherepositoryexhibitananalogousissue:their FROM linesindicatean imagetagnamethatmaychangeontheserverside(figure21.2).Topreventtheseimages fromsilentlychanging,theseshouldbepinnedwithaSHA256hash. hasheye 50ElixirProtocolSecurityAssessment PUBLIC

FROMpython:3.10.12-slim-buster Figure21.2:AnexampleDockerfileusingathird-partyimagereferencedbyitstag (elixir-protocol/services/feed_aggregator/Dockerfile#L1) ExploitScenario Anattacker(orcompromisedmaintainer)silentlyreplacesthe v5 tagonthe stefanzweifel/git-auto-commit-action repositorywithamaliciousactionthat injectsmaliciouscodeintotherepository.Whenthe“GenerateABIs”workflowisrun, maliciouscodeiscommittedanduploadedtotherepository. Recommendations Shortterm,replacethecurrentversiontagreferencesusedintheworkflowforthird-party actionswithfull-lengthcommithashes.Similarly,pinDockerbaseimagesbytheirfull hashes. Longterm,useDependabot’ssupportforGitHubActionstokeepthird-partyactioncommit hashesuptodate,complementedwithmaintainerreviewstoensuretheirsafety. IncorporatestaticanalysistoolssuchasSemgrepintotheCIpipelinetodetectissues earlieron. hasheye 51ElixirProtocolSecurityAssessment PUBLIC

22.AbsenceofaccesscontrolsonpoolcreationfunctionSeverity:InformationalDifficulty:Low Type:AccessControlsFindingID:TOB-ELIXIR-22 Target: protocol/contracts/src/PoolManager.sol Description Poolsactasaformofon-chaindatastorage,withthe poolManager contractresponsible formaintainingtherecordofconfigurationchangesovertime.The createPool functionis usedtocreateandaddnewpools(records)tothecontract’sstorage.However,this functioncurrentlylacksproperaccesscontrols,allowinganyusertocreateandaddnew pools. 85functioncreatePool(86address_baseToken, 87address_quoteToken, 88IPool.Exchange_exchange, 89bytes32_strategy, 90stringcalldata_params 91)externalreturns(addresspool){ 92//GetERC20instanceofbaseTokentogetdecimals. 93ERC20baseToken=ERC20(_baseToken); 94ERC20quoteToken=ERC20(_quoteToken); 95 96//Definepoolparameters 97PoolConstants.PoolParamsmemoryPoolParameters= PoolConstants.PoolParams({ 98owner:msg.sender,//Ownerofpool 99baseToken:baseToken,//Tokentobepaid 100quoteToken:quoteToken,//Tokentobereceived 101exchange:_exchange,//Exchange 102strategy:_strategy,//Strategy 103params:_params//Parameters 104}); 105 106//Createpoolandsaveitsaddress 107pool=address(newPool(abi.encode(PoolParameters))); 108pools.push(pool); 109 110emitPoolCreated(pool,PoolParameters); 111} Figure22.1: contracts/src/PoolManager.sol#L85-L111 Thiscouldexposetheprotocoltopotentialissues: hasheye 52ElixirProtocolSecurityAssessment PUBLIC

- Itallowsuserstosubmitgarbagepooldatatothecontract. - Itcreatesanopportunityforrecreatingexistingpoolswithpotentiallyincorrectdata orparameters. - Legitimatepoolcreationtransactionscanbefront-runwithfakeoneswithsimilar datatotricktheoff-chainmonitoringcomponentintoconsumingthemaliciously alteredpooldata. Recommendations Shortterm,consideraddingtheappropriateaccesscontrolstothe createPool function. Longterm,carefullyreviewallcriticalfunctionswithinthecontractstoensurecorrect accesscontrolsareinplace,andaddconfirmationteststoverifythesafeguardsinplace. hasheye 53ElixirProtocolSecurityAssessment PUBLIC

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 54ElixirProtocolSecurityAssessment PUBLIC

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 55ElixirProtocolSecurityAssessment PUBLIC

B.CodeMaturityCategories
Thefollowingtablesdescribethecodematuritycategoriesandratingcriteriausedinthis document.
CodeMaturityCategories CategoryDescription
ArithmeticTheproperuseofmathematicaloperationsandsemantics
AuditingTheuseofeventauditingandloggingtosupportmonitoring Authentication/ AccessControls
Theuseofrobustaccesscontrolstohandleidentificationand authorizationandtoensuresafeinteractionswiththesystem Complexity Management
Thepresenceofclearstructuresdesignedtomanagesystemcomplexity, includingtheseparationofsystemlogicintoclearlydefinedfunctions
ConfigurationTheconfigurationofsystemcomponentsinaccordancewithbest practices Cryptographyand KeyManagement Thesafeuseofcryptographicprimitivesandfunctions,alongwiththe presenceofrobustmechanismsforkeygenerationanddistribution
DataHandlingThesafehandlingofuserinputsanddataprocessedbythesystem
DecentralizationThepresenceofadecentralizedgovernancestructureformitigating insiderthreatsandmanagingrisksposedbycontractupgrades
DocumentationThepresenceofcomprehensiveandreadablecodebasedocumentation Low-Level Manipulation Thejustifieduseofinlineassemblyandlow-levelcalls
MaintenanceThetimelymaintenanceofsystemcomponentstomitigaterisk MemorySafety andErrorHandling Thepresenceofmemorysafetyandrobusterror-handlingmechanisms Testingand Verification Thepresenceofrobusttestingprocedures(e.g.,unittests,integration tests,andverificationmethods)andsufficienttestcoverage Transaction Ordering Thesystem’sresistancetotransaction-orderingattacks hasheye 56ElixirProtocolSecurityAssessment PUBLIC

RatingCriteria RatingDescription StrongNoissueswerefound,andthesystemexceedsindustrystandards.
SatisfactoryMinorissueswerefound,butthesystemiscompliantwithbestpractices.
ModerateSomeissuesthatmayaffectsystemsafetywerefound.
WeakManyissuesthataffectsystemsafetywerefound.
MissingArequiredcomponentismissing,significantlyaffectingsystemsafety.
NotApplicableThecategoryisnotapplicabletothisreview.
NotConsideredThecategorywasnotconsideredinthisreview. Further Investigation Required Furtherinvestigationisrequiredtoreachameaningfulconclusion. hasheye 57ElixirProtocolSecurityAssessment PUBLIC

C.CodeQualityRecommendations
Thefollowingrecommendationsarenotassociatedwithanyspecificvulnerabilities.
However,theywillenhancecodereadabilityandmaypreventtheintroductionof vulnerabilitiesinthefuture. ● Unuseddependencies.Thefollowingcontractsareinheritedbutneverused. Reviewtheseandre-assesswhethertheyarerequired. ○ PoolManager.ReentrancyGuard ○ Pool.ReentrancyGuard ○ ELX.ERC20VotesUpgradeable ● Error-proneconstants.TheFeeConstantslibrarydefinesa DEFAULT_FEE_TIMESLICE_SECONDS constantequaltothenumberofsecondsper week.Solidityprovidesacollectionofsuffixesthatallowsonetodefinesuch constantsinawaythatislesserrorproneandeasiertoread.Considerreplacingthe value 604800 with 1weeks . ● Unusedstoragevariableandsetterfunction.The minimumStakeAmount state variableanditssetterfunctionaredefinedinthe Core contractbutarenotused. Carefullyreviewtheseandremoveanydeadorunusedcode.
126 ///@noticeSetstheminumumstakeamounttobecomeavalidator.
127 ///@paramnewMinimumStakeAmountStakeamount.
128functionsetMinimumStakeAmount(uint256newMinimumStakeAmount) 129external
130onlyRole(RoleConstants.STAKE_MANAGER_ADMIN) 131{ 132minimumStakeAmount=newMinimumStakeAmount;
133emitMinimumStakeAmountUpdated(newMinimumStakeAmount); 134} FigureC.1:
contracts/src/Core.sol#L126-L134 ● Extractrepeatedlogicintoahelperfunction.The penalizeValidator

method ofthe DisputeManager contracthashighcyclomaticcomplexity.Itcanbe simplifiedbycallingahelperfunctioninsteadofrepeatingthefollowinglogic. //Signermustbeavalidator. boolisValidator=false; //Checkthattheproofsignerisavalidatorandnotjailed. for(uint256j=0;j<consensus.validatorsEnrolled.validators.length;j++){ if(consensus.validatorsEnrolled.validators[j]==proofSigner){ isValidator=true; break; hasheye 58ElixirProtocolSecurityAssessment PUBLIC

} } FigureC.2:Logicfromthe penalizeValidator methodthatcouldbeextractedintoan internalhelpermethod • ReviewandcorrectPythontypinghints.Weobservedseveralinstancesinthe codebasewhereafunctionhasanoptionalargumentwitha None defaultvalue; however,itstypeindicatesitcannotbe None .FigureC.2showsonesuchexample. ThiscanconfusetypecheckersandIDEsand,forinstance,resultinincorrectdead codehighlighting.Use typing.Optional (orthenewer X|None syntax)to conveytypescorrectly. asyncdefproduce_message(self,message:Any,topic_name:str=None,key:str= None,headers:Any=None): iftopic_nameisNone: topic_name=generate_topic_name(category=self.producer_topic_name) ifkeyisNone: key=generate_message_key() FigureC.3:Both topic_name and key aretypedasstrings;however,theirdefaultvalueisnota string(elixir-protocol/shared/shared/event_bus/async_producer.py#32-37) • Preferusingsys.exit(...)overexit(...)whenexitingtheprogram.The exit(...) functionisahelperfortheinteractiveshellandmaynotbeavailableon allPythonimplementations. • Quotevariableusesinshellscriptswheresplittingisundesirable.Variable expansionsmustbedouble-quotedsoastopreventbeingsplitintomultiplepieces accordingtowhitespaceorwhicheverseparatorisspecifiedbytheIFSvariable. • Use apt-get insteadof apt .SeveralDockerfilesinvoke apt toperformpackage management. apt isanend-usertoolanditscommandlineinterfacestabilityisnot guaranteed.Using apt-get ispreferredwhenscripting,asitretainsbackwards compatibility. • Alwaysperform apt-getupdate togetherwiththe apt-getinstall command.Runningthecommandsseparatelymaycauseissuesorleadto out-of-datepackageinstallsduetolayercaching. • Correcttheuseofgetattr(...)defaultvalueswhensortingvalidatorsand rewards.Ifthespecifiedproperty(secondargument)isnotfoundontheobject (firstargument),thedefaultvalue(thirdargument)isreturnedinstead.However, thisargumentisnotareplacementproperty,butadefaultvalue.Considerreplacing theinstancesinfiguresC.3andC.4with validator.apy and reward.amount , respectively. hasheye 59ElixirProtocolSecurityAssessment PUBLIC

sorted_validators=sorted(validators, key=lambdavalidator:getattr(validator,order_by,"apy"), reverse=order_dir=="desc",) FigureC.4:If order_by doesnotdescribeavalidpropertyof validator ,thestring “apy” will beusedforthesortcomparisons. (elixir-protocol-api/app/api/services/validator.py#46-50) sorted_rewards=sorted(rewards, key=lambdareward:getattr(reward,order_by,"amount"), reverse=order_dir=="desc",) FigureC.5:If order_by doesnotdescribeavalidpropertyof reward ,thestring “amount” will beusedforthesortcomparisons. (elixir-protocol-api/app/api/services/rewards.py#57-61) hasheye 60ElixirProtocolSecurityAssessment PUBLIC

D.AutomatedAnalysisToolConfiguration

Thisappendixdescribesthesetupoftheautomatedanalysistoolsusedduringthisaudit. Thoughstaticanalysistoolsfrequentlyreportfalsepositives,theydetectcertaincategories ofissues,suchasmemoryleaks,misspecifiedformatstrings,andtheuseofunsafeAPIs, withessentiallyperfectprecision.Werecommendperiodicallyrunningthesestaticanalysis toolsandreviewingtheirfindings. Slither ToinstallSlither,weused pip byrunning python3-mpipinstallslither-analyzer . WeusedSlithertodetectcommonissuesandanti-patternsinthecodebase.Although Slitherdidnotdiscoveranysevereissuesduringthisreview,someinformationaland code-qualityissueswere detected.IntegratingSlitherintotheproject’stestingenvironment canhelpfindotherissuesthatmaybeintroducedduringfurtherdevelopmentandwillhelp improvetheoverallqualityofthesmartcontracts’code. slither.--no-fail-pedantic--exclude='naming-convention,solc-version' --filter-pathslib,script,test FigureD.1:AnexampleSlitherconfiguration Integrating slither-action intotheproject’sCIpipelinecanautomatethisprocess. Bandit ToinstallBandit,weused pip byrunning python3-mpipinstallbandit . AfterinstallingBandit,weusedthefollowingcommandtoanalyzebothrepositories: bandit-rrepository-folder/ Asthismayresultinmanyfindings,itispossibletoignoresomeofthecodebyusingthe -x flaginBandit.Thefollowingexampleignoresthe scripts.py andtestfiles,aswellasthe defaultBanditignoreset: banditargets/-r-x ".svn,CVS,.bzr,.hg,.git,__pycache__,.tox,.eggs,*.egg,tests,script s.py" Semgrep ToinstallSemgrep,weused pip byrunning python3-mpipinstallsemgrep . hasheye 61ElixirProtocolSecurityAssessment PUBLIC

TorunSemgreponthecodebases,weranthefollowingcommandintherootdirectory containingtheprojects(runningmultiplepredefinedrulessimultaneouslybyproviding multiple --config arguments): semgrep--config"p/hasheye"--config"p/ci"--config"p/python" --config"p/security-audit"--metrics=off Wealsoused semgrep-rules-manager tofetchandrunotherthird-partyrules. WerecommendintegratingSemgrepintotheproject'sCI/CDpipeline.Tothoroughly understandtheSemgreptool,refertothehasheyeTestingHandbook,whereweaimto streamlinetheuseofSemgrepandimprovesecuritytestingeffectiveness.Also,consider doingthefollowing: • Limitresultstoerrorseverityonlybyusingthe --severityERROR flag. • Focusfirstonruleswithhighconfidenceandmedium-orhigh-impactmetadata. • UsetheSARIFformat(byusingthe --sarif Semgrepargument)withtheSARIF ViewerforVisualStudioCodeextension.Thiswillmakeiteasiertoreviewthe analysisresultsanddrilldownintospecificissuestounderstandtheirimpactand severity. CodeQL WeinstalledCodeQLbyfollowingCodeQL'sinstallationguide. AfterinstallingCodeQL,weranthefollowingcommandtocreatetheprojectdatabasefor theElixirrepositories: codeqldatabasecreateelixir.db--language=python Wethenranthefollowingcommandtoquerythedatabase: codeqldatabaseanalyzeelixir.db--format=sarif-latest --output=codeql_res.sarif--python-lgtm-full python-security-and-qualitypython-security-experimental FormoreinformationaboutCodeQL,refertotheCodeQLchapterofthehasheye TestingHandbook. hasheye 62ElixirProtocolSecurityAssessment PUBLIC

E.MutationTesting Mutationtestsmakechangestoeachlineofatargetcontract'ssourcecodeandre-runthe testsuiteagainsteachchange.Changesthatresultintestfailuresindicateadequatetest coverage,whilechangesthatdonotcauseteststofailindicategapsintestcoverage. Mutationtestingallowsauditorstofocustheirreviewonareasofthecodebasethatare mostlikelytocontainlatentbugs,andithelpsdevelopersidentifyandaddmissingtests. Slitherversion0.10.2introducedabuilt-inSoliditymutationtestingtoolwithfirst-class supportforFoundryprojects.Weranamutationtestingcampaignagainstthetargetsmart contractsusingthefollowingcommand: slither-mutate./contracts/src\ --test-cmd='forgetest'\ --ignore-dirs='interfaces,constants' FigureE.1:Acommandthatrunsamutationtestingcampaign againstallsmartcontractsinthe protocol repository Notethattheoverallruntimeofthiscampaignisapproximately40minutesona consumer-gradelaptop.Anabbreviated,illustrativeexampleofamutationtestoutputfile isshowninfigureE.2. INFO:Slither-Mutate:MutatingcontractPoolManager INFO:Slither-Mutate: [RR]Line125:'returnpools'⟹'revert()'⟶UNCAUGHT INFO:Slither-Mutate: [CR]Line62:'_disableInitializers()'⟹ '//_disableInitializers()'⟶UNCAUGHT INFO:Slither-Mutate: [CR]Line71:'__UUPSUpgradeable_init()'⟹ '//__UUPSUpgradeable_init()'⟶UNCAUGHT INFO:Slither-Mutate:[CR]Line110:'emitPoolCreated(pool,PoolParameters)'⟹ '//emitPoolCreated(pool,PoolParameters)'⟶UNCAUGHT INFO:Slither-Mutate: [CR]Line120:'emitPoolUpdated(address(pool),params)'⟹ '//emitPoolUpdated(address(pool),params)'--›UNCAUGHT ERROR:Slither-Mutate:listindexoutofrange INFO:Slither-Mutate:DonemutatingPoolManager. INFO:Slither-Mutate:Revertmutants:1uncaughtof9(11.1111111111111%) INFO:Slither-Mutate:Commentmutants:4uncaughtof8(50.0%) INFO:Slither-Mutate:ZeroTweakmutantsanalyzed FigureE.2:Abbreviatedoutputfromthemutationtesting campaignon PoolManager.sol Insummary,thefollowingfeaturesofthe PoolManager contractlacksufficienttests: • The pools gettermethodisnotexecutedbyanytests,asindicatedbytheuncaught revertmutantonline125. hasheye 63ElixirProtocolSecurityAssessment PUBLIC

• Notestsvalidatetheinitializationlogicofimplementationandproxycontracts. Whenimportantdeploymentstepsarecommentedoutonlines62and71,thetests stillpass. • Eventemissions,suchasthoseonlines110and120,arenotvalidatedbytests. WerecommendthattheElixirteamreviewtheexistingtestsandaddadditionalverification thatwouldcatchtheaforementionedtypesofmutations.Then,useascriptsimilartothat providedinfigureE.1tore-runamutationtestingcampaigntoensurethattheaddedtests provideadequatecoverage. hasheye 64ElixirProtocolSecurityAssessment PUBLIC

F.IncidentResponseRecommendations Thissectionprovidesrecommendationsonformulatinganincidentresponseplan. • Identifytheparties(eitherspecificpeopleorroles)responsiblefor implementingthemitigationswhenanissueoccurs(e.g.,deployingsmart contracts,pausingcontracts,upgradingthefrontend,etc.). • Documentinternalprocessesforaddressingsituationsinwhichadeployed remedydoesnotworkorintroducesanewbug. ○ Considerdocumentingaplanofactionforhandlingfailedremediations. • Clearlydescribetheintendedcontractdeploymentprocess. • Outlinethecircumstancesunderwhich ElixirTechnologiesLtdwill compensateusersaffectedbyanissue(ifany). ○ Issuesthatwarrantcompensationcouldincludeanindividualoraggregate

lossoralossresultingfromusererror,acontractflaw,orathird-party contractflaw. ● Documenthowtheteamplanstostayuptodateonnewissuesthatcould affectthesystem;awarenessofsuchissueswillinformfuturedevelopment workandhelptheteamsecurethedeploymenttoolchainandtheexternal on-chainandoff-chainservicesthatthesystemrelieson. ○ Identifysourcesofvulnerabilitynewsforeachlanguageandcomponentused inthesystem,andsubscribetoupdatesfromeachsource.Considercreating aprivateDiscordchannelinwhichabotwillpostthelatestvulnerability news;thiswillprovidetheteamwithawaytotrackallupdatesinoneplace. Lastly,considerassigningcertainteammemberstotracknewsabout vulnerabilitiesinspecificsystemcomponents. ● Determinewhentheteamwillseekassistancefromexternalparties(e.g., auditors,affectedusers,otherprotocoldevelopers)andhowitwillonboard them. ○ Effectiveremediationofcertainissuesmayrequirecollaborationwith externalparties. ● Definecontractbehaviorthatwouldbeconsideredabnormalbyoff-chain monitoringsolutions. hasheye 65ElixirProtocolSecurityAssessment PUBLIC

Itisbestpracticetoperformperiodicdryrunsofscenariosoutlinedintheincident responseplantofindomissionsandopportunitiesforimprovementandtodevelop “musclememory.”Additionally,documentthefrequencywithwhichtheteamshould performdryrunsofvariousscenarios,andperformdryrunsofmorelikelyscenariosmore regularly.Createatemplatetobefilledoutwithdescriptionsofanynecessary improvementsaftereachdryrun. hasheye 66ElixirProtocolSecurityAssessment PUBLIC

G.SecurityBestPracticesforUsingMultisignature Wallets Consensusrequirementsforsensitiveactions,suchasupgradingcontracts,aremeantto mitigatetherisksofthefollowing: ● Anyonepersonoverrulingthejudgmentofothers ● Failurescausedbyanyoneperson’smistake ● Failurescausedbythecompromiseofanyoneperson’scredentials Forexample,ina2-of-3multisignaturewallet,theauthoritytoupgradethe StakeManager contractwouldrequireaconsensusoftwoindividualsinpossessionoftwoofthewallet’s threeprivatekeys.Forthismodeltobeuseful,thefollowingconditionsarerequired: 1.Theprivatekeysmustbestoredorheldseparately,andaccesstoeachonemustbe limitedtoauniqueindividual. 2.Ifthekeysarephysicallyheldbythird-partycustodians(e.g.,abank),multiplekeys shouldnotbestoredwiththesamecustodian.(Doingsowouldviolaterequirement #1.) 3.Thepersonaskedtoprovidethesecondandfinalsignatureonatransaction(i.e., thecosigner)shouldrefertoapre-establishedpolicyspecifyingtheconditionsfor approvingthetransactionbysigningitwithhisorherkey. 4.Thecosignershouldalsoverifythatthehalf-signedtransactionwasgenerated willinglybytheintendedholderofthefirstsignature’skey. Requirement#3preventsthecosignerfrombecomingmerelya“deputy”actingonbehalf ofthefirstsigner(forfeitingthedecision-makingresponsibilitytothefirstsignerand defeatingthesecuritymodel).Ifthecosignercanrefusetoapprovethetransactionforany reason,thedue-diligenceconditionsforapprovalmaybeunclear.Thatiswhyapolicyfor validatingtransactionsisneeded.Averificationpolicycouldincludethefollowing: ● Aprotocolforhandlingarequesttocosignatransaction(e.g.,ahalf-signed transactionwillbeacceptedonlyviaanapprovedchannel) ● Anallowlistofspecificaddressesallowedtobethepayeeofatransaction ● Alimitontheamountoffundsspentinasingletransactionorinasingleday hasheye 67ElixirProtocolSecurityAssessment PUBLIC

Requirement#4mitigatestherisksassociatedwithasinglestolenkey.Forexample,say thatanattackersomehowacquiredtheunlockedLedgerNanoSofoneofthesignatories. Avoicecallfromthecosignertotheinitiatingsignatorytoconfirmthetransactionwould revealthatthekeyhadbeenstolenandthatthetransactionshouldnotbecosigned.Ifthe signatorywereunderanactivethreatofviolence,heorshecoulduseaduresscode(a codeword,aphrase,oranothersignalagreeduponinadvance)tocovertlyalerttheothers thatthetransactionhadnotbeeninitiatedwillingly,withoutalertingtheattacker. hasheye 68ElixirProtocolSecurityAssessment PUBLIC

H.FixReviewResults Whenundertakingafixreview,hasheyereviewsthefixesimplementedforissues identifiedintheoriginalreport.Thisworkinvolvesareviewofspecificareasofthesource codeandsystemconfiguration,notcomprehensiveanalysisofthesystem. OnSeptember6,2024,hasheyereviewedthefixesandmitigationsimplementedbythe ElixirTechnologiesLtd.teamfortheissuesidentifiedinthisreport.Wereviewedeachfixto determineitseffectivenessinresolvingtheassociatedissue. Insummary,allofthe22issuesdescribedinthisreportwereresolvedbyElixir TechnologiesLtd.Foradditionalinformation,pleaseseetheDetailedFixReviewResults below. IDTitleStatus

1UseofoutdateddependenciesResolved 2UseofHTTPrequestswithouttimeoutResolved
3PrivatekeysstoredinenvironmentvariablesResolved 4Majorityproposalgroupwillalwayssatisfyminimumsize
requirement Resolved 5AuthenticationatriskofreplayattacksifmisconfiguredResolved
6StrategyexecutordoesnotvalidatepayloadtosignResolved
7MissingIPaddressvalidationallowsbypassingRedpandaACLResolved
8UseofassertstatementinproductioncodeResolved
9RedpandaaccountsandassociatedpermissionsareneverrevokedResolved
10DelegatorscanredelegatestakestojaileddelegateeResolved
11AttackerscancauseslashingtobecomeeconomicallyinfeasibleResolved hasheye
69ElixirProtocolSecurityAssessment PUBLIC

12Delegatorscanimmediatelyundelegatebeforetheirdelegateeis jailed Resolved
13MinorityvalidatorsmayparticipateinconsensusprocessResolved
14AninfluxofnewstrategyexecutorsmayhaltconsensusResolved 15Lackoftwo-
stepprocessforownershiptransfersResolved
16ResponsepayloadtoauthenticationchallengeisnotsignedResolved
17APIdoesnotvalidatedisplay_nameandapp_versionResolved 18Allon-
chaineventsreplayeduponstartupResolved 19RedpandaexposedtotheInternetResolved
20APIhasadminaccesstoRedpandaResolved 21Useofunpinnedthird-
partyDockerimagesandactionsonworkflowsResolved
22AbsenceofaccesscontrolsonpoolcreationfunctionResolved hasheye 70ElixirProtocolSecurityAssessment
PUBLIC

DetailedFixReviewResults TOB-ELIXIR-1:Useofoutdateddependencies
ResolvedinPR465.ThePythondependencieswereupdated. TOB-ELIXIR-2:UseofHTTPrequestswithouttimeout
Resolvedincommit6c0031d.A45-secondtimeoutwasaddedtotherequests. TOB-ELIXIR-
3:Privatekeysstoredinenvironmentvariables
ResolvedinPR572,PR478,andPR549.TheservicesnowissuesignrequeststoGoogle
CloudKeyManagementServicewheretheprivatekeymaterialisstored.Thevalidatorsare
providedwithmultipleoptionsforkeymaterialstorage,includingthemanagedcloud solutions.Theless-
safemethodsarestillavailable,althoughtheyarediscouragedbecause
theElixirProtocolteamhasnocontroloverthevalidatorsruntimeenvironment.We
recommenddocumentingallthekeymanagementoptionssotheusersareawareofthe risks. TOB-ELIXIR-
4:Majorityproposalgroupwillalwayssatisfyminimumsizerequirement
Resolvedincommita949bc1.Thecalculationof minimum_requirement wasfixedand nowisafractionofthe
total_proposals . TOB-ELIXIR-5:Authenticationatriskofreplayattacksifmisconfigured
Resolvedincommit481a55a.Thecodewasrefactored,andtheRedisserviceisinjectedas
adependency.Thenonceisnolongeremptywhenserviceismisconfigured. TOB-ELIXIR-
6:StrategyexecutordoesnotvalidatepayloadtosignResolvedinPR474.Themessagestructurevalidationwasaddedtothestrategyexecutor code. TOB-ELIXIR-
7:MissingIPaddressvalidationallowsbypassingRedpandaACL
Resolvedincommits0dbd7d6and38db652.Thearchitecturehaschanged,andIP
addressesarenolongercollectedfromvalidators,removingtheneedforvalidation. TOB-ELIXIR-
8:UseofassertstatementinproductioncodeResolvedinPR487.Theassertstatementswerereplacedwithexplicitraisestatements
underviolatingconditions. TOB-ELIXIR-9:RedpandaaccountsandassociatedpermissionsareneverrevokedResolvedinPR42.Thearchitecturehaschanged,andAPInolongerconfiguresthe
RedpandaACLs.Theaccessrevocationmechanismisnolongerneeded. TOB-ELIXIR-
10:DelegatorscanredelegatestakestojaileddelegateeResolvedincommita0ae84e.Anadditionalcheckhasbeenaddedtothe _updateDelegation
methodthatpreventsauserfromdelegatingtoanaddressthathas beenjailed. hasheye
71ElixirProtocolSecurityAssessment PUBLIC

TOB-ELIXIR-11:AttackerscancauseslashingtobecomeeconomicallyinfeasibleResolvedincommitfd18709.The
slash methodofthe Core contractnowacceptsalistof
accountsandlistofamounts,respectively,toslash,withappropriateverificationoflist
lengths.Thisdecreasesthegasoverheadfromslashingalargenumberofaccounts.
Werecommendfurtheranalysisofgasusage.Reviewtheshort-termrecommendationfor
thisissueandconsiderwhetheritwouldbeacceptabletoslashthebalanceofaccounts
downtozeroifandonlyifaccountsareflaggedasmisbehavinginthespecificway
describedbythisissue.Doingsowouldsignificantlylowerthegasusageofslashingmany
accountsinsuchscenarios. TOB-ELIXIR-12:DelegatorscanimmediatelyundelegatebeforetheirdelegateeisResolvedincommitaf5634d.Eventlistenersinthe onchain_stake_manager_feed servicenowrespondto
SignalRedelegate and CancelSignalRedelegate events. Whena SignalRedelegate
eventisreceived,thecurrentdelegatedbalanceissubtracted
fromtheexistingdelegatedbalance,andthisdelegatorisremovedfromthelistofstaker

addresses(onlyifthisdelegatorhasnotalreadybeenremoved).Thiscausesdelegators thathavesignaledanintenttoredelegatetobeexcludedfromavalidator’stotal delegations.Additionally,whena CancelSignalRedelegate eventisreceived,thisaction isundonebyaddingthedelegatedbalancebacktotheolddelegateeandaddingtheir addressbacktothelistofstakeraddresses. Critically,the StakeManager contractwasupdatedinPR689toallowsignalcancellations onlywhenasignalhasbeenregisteredbutthesignaledactionhasnotyetbeencompleted. Thiswillpreventamalicioususerfromrepeatedlycancelingsignalstorepeatedlyincrease theirdelegatedbalance. TOB-ELIXIR-13:MinorityvalidatorsmayparticipateinconsensusprocessResolvedinPR497andPR42.Thevalidatorsystemhasbeenrearchitected,anditisno longerpossibletosubmitaproposalwithoutbeinginthecorevalidatorset. TOB-ELIXIR-14:AninfluxofnewstrategyexecutorsmayhaltconsensusResolvedinPR497andPR42.Theconstraintisnowafractionofthecorevalidatorsetsize, whichsolvestheissuewithconsensushaltingbyaninfluxofmaliciousvalidators. TOB-ELIXIR-15:Lackoftwo-stepprocessforownershiptransfers Resolvedincommit543b3e0.The OwnableUpgradeable dependencieshavebeen replacedwith Ownable2StepUpgradeable contractsthatproperlyimplementatwo-step processforownershiptransfers. hasheye 72ElixirProtocolSecurityAssessment PUBLIC

TOB-ELIXIR-16:ResponsepayloadtoauthenticationchallengeisnotsignedResolvedinPR56.Therequeststructurewasrefactoredinto ValidatorAuthorizationRequest ,whichcontainsaproofanddetail.Thedetail structureisencodedwithEthereumABIforsignatureverification. TOB-ELIXIR-17:APIdoesnotvalidatedisplay_nameandapp_versionResolvedinPR42.Thevaluesarenowvalidatedintheapplicationcodeaswellasinthe database. TOB-ELIXIR-18:Allon-chaineventsreplayeduponstartupResolvedinPR498.Theservicesnowresumeeventconsumptionfromthelastprocessed eventinsteadofreplayingthehistoryfromthebeginningonstartup. TOB-ELIXIR-19:RedpandaexposedtotheInternetResolvedinPR42.ThebackendwasrearchitectedinsuchawaythatRedpandaissplitinto twoclusters,oneontheinternalnetworkandonethatisinternet-facing.The internet-facingclusterisread-only,andvalidatorsdonotwriteanydatatoit.Theorder proposalsarenowsenttotheAPI.AlthoughthisfixwasnotpartofouroriginalrecommendationandRedpandaisstillexposed,thenewarchitectureminimizesthe possibledamagetothepointweconsideritresolved. TOB-ELIXIR-20:APIhasadminaccesstoRedpandaResolvedinPR42andcommit8de6fdd.Thearchitecturehaschanged,andtheAPIno longerconfigurestheRedpandaACLs.Theadminaccessandrelatedcodewasremoved fromtheservice. TOB-ELIXIR-21:Useofunpinnedthird-partyDockerimagesandactionsonworkflowsResolvedincommitsc4360ebandf34b570.Third-partyDockerimagesandactionswere pinned. TOB-ELIXIR-22:AbsenceofaccesscontrolsonpoolcreationfunctionResolvedincommit0d15c2f.An onlyOwner functionmodifierhasbeenaddedtothe createPool methodofthe PoolManager contract. hasheye 73ElixirProtocolSecurityAssessment PUBLIC

I.FixReviewStatusCategories

Thefollowingtabledescribesthestatusesusedtoindicatewhetheranissuehasbeen sufficientlyaddressed.

FixStatus StatusDescription UndeterminedThestatusoftheissuewasnotdeterminedduringthisengagement.

UnresolvedTheissuepersistsandhasnotbeenresolved.

PartiallyResolvedTheissuepersistsbuthasbeenpartiallyresolved.

ResolvedTheissuehasbeensufficientlyresolved. hasheye 74ElixirProtocolSecurityAssessment PUBLIC