HashEye

// SMART CONTRACT SECURITY AUDIT

Orbit

Security assessment by HashEye · prepared for AppSec

HASHEYE AUDITED

PROJECT	Orbit
CLIENT	AppSec
CATEGORY	Blockchain
PUBLISHED	April 1, 2021
REPORT ID	research-orbit-2021-04-01-00mta2

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-orbit-2021-04-01-00mta2.

OrbitandGovernanceUpgrade Actionsv2.1 SecurityAssessment August29,2024 Preparedfor: OffchainLabs Preparedby:GustavoGrieco

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 1OffchainLabsOrbitActionsSecurityAssessment PUBLIC

NoticesandRemarks CopyrightandDistribution ©2024byhasheye,Inc. Allrightsreserved.hasheyeherebyassertsitsrighttobeidentifiedasthecreatorofthis reportintheUnitedKingdom. Thisreportisconsideredbyhasheyetobepublicinformation;itislicensedtoOffchain Labsunderthetermsoftheprojectstatementofworkandhasbeenmadepublicat OffchainLabs'request.Materialwithinthisreportmaynotbereproducedordistributedin partorinwholewithouttheexpresswrittenpermissionofhasheye. 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 2OffchainLabsOrbitActionsSecurityAssessment PUBLIC

ProjectSummary ContactInformation Thefollowingprojectmanagerwasassociatedwiththisproject: MaryO'Brien,ProjectManager mary.obrien@hasheye.io Thefollowingengineeringdirectorwasassociatedwiththisproject: JosselinFeist,EngineeringDirector,Blockchain josselin.feist@hasheye.io Thefollowingconsultantswereassociatedwiththisproject: GustavoGrieco,Consultant gustavo.grieco@hasheye.io ProjectTimeline Thesignificanteventsandmilestonesoftheprojectarelistedbelow. DateEvent August9,2024Pre-

projectkickoffcall August16,2024Deliveryofreportdraft August29,2024Deliveryofcomprehensivereport hasheye 4OffchainLabsOrbitActionsSecurityAssessment PUBLIC

ExecutiveSummary EngagementOverview OffchainLabsengagedhasheyetoreviewthesecurityoftheirOrbitgovernanceactions forvariousupgrades.Theupgradesincludedinthisauditareupdatingthewasmroothash; upgradingtherollupcontractstoversion0.2.1;increasingthetimedelayforgovernance actions;enablingthefastconfirmcommittee;andmigratinganypreviousAnyTrustfast confirmer. AteamofoneconsultantconductedthereviewfromAugust12,2024toAugust16,2024, foratotalofoneengineer-weekofeffort.Ourtestingeffortsfocusedonthemanualreview ofthecodethatperformstheupgradeactions. ObservationsandImpact TheidentifiedissuesrelatetotheincorrectusageofaGnosisSafemultisig.Inparticular, TOB-ORBUPG-001allowsexternaluserstoblockanupgrade,requiringredeploymentof theactioncontracttocompletetheupgrade. Recommendations Basedonthecodebasematurityevaluationandfindingsidentifiedduringthesecurity review,hasheyerecommendsthatOffchainLabstakethefollowingsteps: • Carefullymonitortheblockchainduringthedeploymentandexecutionof upgradeactions.Althoughtheuseofanadditionalsaltvalueonthedeployment mitigatesTOB-ORBUPG-001,front-runningthetransactionispossibleincertain cases. • ProperlydocumenthowchainownersshoulduseGnosisSafemultisigfor implementingafastconfirmationcommittee.Thiswillavoidfutureissuesduring deploymentandusageofthisthird-partycomponent. FindingSeveritiesandCategories Thefollowingtablesprovidethenumberoffindingsbyseverityandcategory. hasheye 5OffchainLabsOrbitActionsSecurityAssessment PUBLIC

EXPOSUREANALYSIS SeverityCount High0 Medium1 Low0 Informational1 CATEGORYBREAKDOWN CategoryCount Configuration1 Timing1 hasheye 6OffchainLabsOrbitActionsSecurityAssessment PUBLIC

ProjectGoals TheengagementwasscopedtoprovideasecurityassessmentoftheOrbitandGovernance UpgradeActionsv2.1.Specifically,wesoughttoanswerthefollowingnon-exhaustivelistof questions: • Isthereanywaytoblockordelaytheexecutionofanupgrade? • Dotheupgradesintroduceanysecurityrisks? • Doesastoragechangeoftheupgradedversionoftherollupcodecreateany potentialissues? • IstheGnosisSafemultisigcorrectlyconfiguredandused? hasheye 7OffchainLabsOrbitActionsSecurityAssessment PUBLIC

ProjectTargets Theengagementinvolvedareviewandtestingofthetargetslistedbelow: OrbitActions Repositoryhttps://github.com/OffchainLabs/orbit-actions/pull/16 https://github.com/OffchainLabs/orbit-actions/pull/19 https://github.com/OffchainLabs/orbit-actions/pull/20 Version b743a21cb1aac7efe50da04dcfa0271c3c3538c8 cc4fc585b1832896d0ed79e457b4dc6003653abc 7157bc16c6505ee3e468bbbe4436df1073c96dee TypeSolidity PlatformEVM GovernanceActions Repositoryhttps://github.com/ArbitrumFoundation/governance/pull/305 https://github.com/ArbitrumFoundation/governance/pull/306 Version e7ffee080a21a0f66b0992f33f3ab885c6b667f3 f616c311cc2294de6ba6c4b44fc3b2029a672e93 TypeSolidity PlatformEVM NitroContracts Repositoryhttps://github.com/OffchainLabs/nitro-contracts/pull/233 Version 22d2f322d827b588659486b4b1cf7f81d771350d TypeSolidity PlatformEVM hasheye 8OffchainLabsOrbitActionsSecurityAssessment PUBLIC

ProjectCoverage Thissectionprovidesanoverviewoftheanalysiscoverageofthereview,asdeterminedby ourhigh-levelengagementgoals.Ourapproachesincludedthefollowing: • UpgradeOrbitcontractsandpermissionlessenablefastconfirmation:Theseprovide anumberofstatechangesintherollup: ○ AllowOrbitchainstoupgradetov2.1.0fromsupportedversions.Only relevantcontracts(i.e., ChallengeManager , OSP , RollupLogics)are upgraded. ○ Configure condOsp tosupportongoingchallengesusingtheold OSP . ○ Additionally,the EnableFastConfirmAction contractprovidesaneasy approachtoenablefastconfirmationbybundlingthesetupofall dependencies. ○ ScheduleArbOS31BiancaupgradeusingtheArbOSupgradeattimestamp action. ○ EnableWASMcachemanagerusingthe AddWasmCacheManagerAction upgradeaction. • UpgradeOrbitcontractsandpermissionedenablefastconfirmationusingaspecific address:Thisactionissimilartothepreviousone,butinsteadofdeployingaGnosis Safemultisig,itenablesfastconfirmationusingaspecificaddress. • Updatesgovernancetimelockdelay:thisactionintroducesaneight-daydelayonthe executionofgovernanceaction,whichallowsuserstowithdrawfundsiftheydonot agreewiththegovernanceaction(orevenifitismalicious). •MigrateanyTrustFastConfirmer,ifanyexists:Thisactionensuresthatany previousAnyTrustfastconfirmerismigrated. CoverageLimitations Becauseofthetime-boxednatureoftestingwork,itiscommontoencountercoverage limitations.Thefollowinglistoutlinesthecoveragelimitationsoftheengagementand indicatessystemelementsthatmaywarrantfurtherreview: •

WedidnotreviewGnosisSafemultisigcode,exceptforthespecificinteractions duringdeploymentoftheupgradeaction. • Wedidnotreviewcodechangesbetweencompatibleupgradeversions(e.g.1.1.0to 2.1.0),exceptfortheireffectonthestatecompatibilityaftertheupgrade. hasheye 9OffchainLabsOrbitActionsSecurityAssessment PUBLIC

SummaryofFindings Thetablebelowsummarizesthefindingsofthereview,includingtypeandseveritydetails. IDTitleTypeSeverity 1Gnosissafedeploymentallowsuserstodisrupt governanceactionexecution TimingMedium 2ThresholdofsignaturesusedinfastConfirmercanbe tooinflexible ConfigurationInformational hasheye 10OffchainLabsOrbitActionsSecurityAssessment PUBLIC

DetailedFindings 1.Gnosissafedeploymentallowsuserstodisruptgovernanceaction execution Severity:MediumDifficulty:Low Type:TimingFindingID:TOB-ORBUPG-001 Target: contracts/parent-chain/fast-confirm/EnableFastConfirmAction.sol Description Anyusercanaccidentallyorintentionallyblocktheusageofa GnosisSafedeploymentto setupafastconfirmercommitteeaspartofthegovernanceaction. ThefastconfirmerconfigurationactiondeploysaGnosisSafemultisiginorderto implementacommitteeofvalidatorstofast-confirmarollupstate: functionperform(IRollupAdminrollup,address[]calldatafastConfirmCommittee) external{ ... addressfastConfirmer= IGnosisSafeProxyFactory(GNOSIS_SAFE_PROXY_FACTORY).createProxyWithNonce(GNOSIS_SAFE_1_3_0, abi.encodeWithSignature("setup(address[],uint256,address,bytes,address,address,uint256,address)", fastConfirmCommittee, fastConfirmCommittee.length, address(0), "", GNOSIS_COMPATIBILITY_FALLBACK_HANDLER, address(0), 0, address(0)), uint256(keccak256(abi.encodePacked(rollup)))); rollup.setAnyTrustFastConfirmer(fastConfirmer); address[]memoryvalidators=newaddress[](1); validators[0]=fastConfirmer; bool[]memoryval=newbool[](1); val[0]=true; rollup.setValidator(validators,val); hasheye 11OffchainLabsOrbitActionsSecurityAssessment PUBLIC

rollup.setMinimumAssertionPeriod(1); } Figure1.1:PartoftheperformfunctionfromtheEnableFastConfirmationaction However,sincethedeploymentisperformedinadeterministicwayusing create2 froma factorycontract,thesaltmustbeuniquetoavoidcollisions.Usingthesamesaltastheone fromanalready-deployedGnosisSafewillcausethisactiontorevert. Theupdatedversionofthecodeincludesasaltvaluethatmitigatesthisissue: functionperform(IRollupAdminrollup,address[]calldatafastConfirmCommittee, uint256salt)external{ ... addressfastConfirmer= IGnosisSafeProxyFactory(GNOSIS_SAFE_PROXY_FACTORY).createProxyWithNonce(GNOSIS_SAFE_1_3_0, abi.encodeWithSignature("setup(address[],uint256,address,bytes,address,address,uint256,address)", fastConfirmCommittee, fastConfirmCommittee.length, address(0), "", GNOSIS_COMPATIBILITY_FALLBACK_HANDLER, address(0), 0, address(0)), salt); Figure1.2:Partofthe perform functionfromthefastconfirmationaction However,westressthatthisisonlyamitigation,asfront-runningthistransactionincertain chainslikeEthereummainnetisstillfeasible. Additionally,inthe UpgradeAndEnableFastConfirmAction action,therollupowner mustperformthedeploymentofthe AnyTrustFast confirmer: functionperform()external{ ... //SetupAnyTrustFastConfirmer require(IRollupAdminFC(rollupAddress).anyTrustFastConfirmer()==address(0), "UpgradeAndEnableFastConfirmAction:Fastconfirmalreadyenabled"); IRollupAdminFC(rollupAddress).setAnyTrustFastConfirmer(anyTrustFastConfirmer hasheye 12OffchainLabsOrbitActionsSecurityAssessment PUBLIC

); require(IRollupAdminFC(rollupAddress).anyTrustFastConfirmer() ==anyTrustFastConfirmer, "UpgradeAndEnableFastConfirmAction:UnexpectedanyTrustFastConfirmer"); //SetAnyTrustFastConfirmerasvalidator address[]memoryvalidators=newaddress[](1); validators[0]=anyTrustFastConfirmer; bool[]memoryvalues=newbool[](1); values[0]=true; IRollupAdmin(rollupAddress).setValidator(validators,values); require(IRollupCore(rollupAddress).isValidator(anyTrustFastConfirmer), "UpgradeAndEnableFastConfirmAction:Failedtosetvalidator"); //Setminimumassertionperiod IRollupAdmin(rollupAddress).setMinimumAssertionPeriod(newMinimumAssertionPeriod); require(IRollupCore(rollupAddress).minimumAssertionPeriod() ==newMinimumAssertionPeriod, "UpgradeAndEnableFastConfirmAction:Failedtosetminimumassertion period"); } Figure1.3:Partofthe perform functionfromthefastconfirmationandupgradeaction Again,ifthedeploymentusesGnosisSafemultisigandanattackerisabletoguessand front-runthedeployment,theresultcouldbecatastrophicfortherollup. ExploitScenario Amalicioususerfront-runsthecreationoftheGnosissafedeployment,blockingthe governanceactionuntilitiscreatedagain. Recommendations Shortterm,carefullymonitortheblockchainduringthedeploymentandexecutionofthis governanceactiontodetectpotentialfront-runningattempts.

Longterm,reviewthesecurityassumptionsandrequirementsforthird-partycodebefore usingitingovernanceactions. hasheye 13OffchainLabsOrbitActionsSecurityAssessment PUBLIC

2.ThresholdofsignaturesusedinfastConfirmerisoverlyinflexible Severity:InformationalDifficulty:High Type:ConfigurationFindingID:TOB-ORBUPG-002 Target: contracts/parent-chain/fast-confirm/EnableFastConfirmAction.sol Description ThefastconfirmercommitteeisimplementedusingaGnosisSafethatusesthemaximum threshold,makingitveryinflexibleifchangesareneeded.

```
functionperform(IRollupAdminrollup,address[]calldatafastConfirmCommittee, uint256salt)external{ ...
addressfastConfirmer= IGnosisSafeProxyFactory(GNOSIS_SAFE_PROXY_FACTORY).createProxyWithNonce(
GNOSIS_SAFE_1_3_0, abi.encodeWithSignature(
"setup(address[],uint256,address,bytes,address,address,uint256,address)", fastConfirmCommittee,
fastConfirmCommittee.length, address(0), "", GNOSIS_COMPATIBILITY_FALLBACK_HANDLER, address(0), 0,
address(0) ), salt ); ... Figure2.1:Partofthe perform functionfromthefastconfirmeraction
```

However,usingthemaximumthresholdwhileprovidingmaximumprotectiontotherollup canbeoverlyinflexible,potentiallypreventingarequiredadministrativeactioninthe GnosisSafeitself. ExploitScenario Amemberofthefastconfirmcommitteehastheirkeyleaked,destroyed,orrevoked.The remainingmembersofthecommitteeareunabletochangetheGnosisSafemultisig configurationsincetheydonotreachthethresholdlimit. hasheye 14OffchainLabsOrbitActionsSecurityAssessment PUBLIC

Recommendations Shortterm,allowchainownerstoselectthethresholdnumber.Thisissuewasfixedand verifiedduringthelastpartofthereview. Longterm,reviewthesecurityassumptionsandrequirementsforthird-partycodebefore usingitingovernanceactions. hasheye 15OffchainLabsOrbitActionsSecurityAssessment 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 16OffchainLabsOrbitActionsSecurityAssessment 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 17OffchainLabsOrbitActionsSecurityAssessment PUBLIC