HashEye

// SMART CONTRACT SECURITY AUDIT

Onchain Pass

Security assessment by HashEye · prepared for Pass App Ltd

HASHEYE AUDITED

PROJECT	Onchain Pass
CLIENT	Pass App Ltd
CATEGORY	Blockchain
PUBLISHED	August 1, 2024
REPORT ID	research-onchain-pass-2024-08-01-13i3cm

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-onchain-pass-2024-08-01-13i3cm.

OnchainPassAppContracts SecurityAssessment(SummaryReport) September10,2024 Preparedfor: ManuSiddalingegowda PassAppLtd. Preparedby:GuillermoLarregay

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 1PassAppLtd.SecurityAssessment PUBLIC

NoticesandRemarks CopyrightandDistribution ©2024byhasheye,Inc. Allrightsreserved.hasheyeherebyassertsitsrighttobeidentifiedasthecreatorofthis reportintheUnitedKingdom. Thisreportisconsideredbyhasheyetobepublicinformation;itislicensedtoPassApp Ltd.underthetermsoftheprojectstatementofworkandhasbeenmadepublicatPass AppLtd'srequest.Materialwithinthisreportmaynotbereproducedordistributedinpart orinwholewithouttheexpresswrittenpermissionofhasheye. 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 2PassAppLtd.SecurityAssessment PUBLIC

TableofContents Abouthasheye1 NoticesandRemarks2 TableofContents3 ProjectSummary4 ProjectTargets5 ExecutiveSummary6 CodebaseMaturityEvaluation8 SummaryofFindings11 A.VulnerabilityCategories12 B.CodeMaturityCategories14 C.TokenIntegrationChecklist16 D.IncidentResponseRecommendations19 E.SecurityBestPracticesforUsingMultisignatureWallets21 F.UpgradabilityCheckswithSlither23 G.FixReviewResults24 DetailedFixReviewResults25 H.FixReviewStatusCategories27 hasheye 3PassAppLtd.SecurityAssessment PUBLIC

ProjectSummary ContactInformation Thefollowingprojectmanagerwasassociatedwiththisproject: SamGreenup,ProjectManager sam.greenup@hasheye.io Thefollowingengineeringdirectorwasassociatedwiththisproject: JosselinFeist,EngineeringDirector,Blockchain josselin.feist@hasheye.io Thefollowingconsultantswereassociatedwiththisproject: GuillermoLarregay,Consultant guillermo.larregay@hasheye.io ProjectTimeline Thesignificanteventsandmilestonesoftheprojectarelistedbelow. DateEvent August5,2024Pre-

projectkickoffcall August13,2024Deliveryofreportdraft August13,2024Reportreadoutmeeting September10,2024Deliveryofsummaryreport hasheye 4PassAppLtd.SecurityAssessment PUBLIC

ProjectTargets Theengagementinvolvedareviewandtestingofthefollowingtarget. PassAppContracts Repositoryhttps://github.com/PassHQ/pass-contracts Versioncommit deb8e33 TypeSolidity PlatformEVMcompatible hasheye 5PassAppLtd.SecurityAssessment PUBLIC

ExecutiveSummary EngagementOverview PassAppLtd.engagedhasheyetoreviewthesecurityofPassAppContractscommit deb8e33 .Thecontractimplementsamultisignature-ownedVaultthatacceptsERC20 tokensandnativeassetsdepositsandwithdrawals.Additionally,thereisaswap functionalitythatperformsswappingandbridgingofassetsusingathird-partyaggregator exchange,andafunctiontofundanexternalpaymaster. Ateamofoneconsultantconductedthereviewfromaugust5toAugust9,2024,foratotal ofoneengineer-weekofeffort.Withfullaccesstosourcecodeanddocumentation,we performedstaticanddynamictestingofthetargetusingautomatedandmanual processes. ObservationsandImpact Theengagementwasscopedtoprovideasecurityassessmentofthe PassAppVault contract.Specifically,wesoughttoanswerthefollowingnon-exhaustivelistofquestions: • Canthefundsbewithdrawnfromthevaultbyanattacker,bypassingtheowner's role? • CantheSwapperperformanyotherprivilegedactionsotherthantheexpected swaps? • Cananexternaluserlockfundsorotherwiseaffecttheowner'sorswapper’sability toaccessthefundsinthevault? Theauditfoundsevenissues:oneofmediumseverity,oneoflowseverity,andthree informationalissues.Theseverityoftheremainingtwoissuescouldnotbedetermined fromtheinformationavailableatthetimeoftheengagement.Inparticular,the medium-severityissue(TOB-PASS-1)couldleadtoanunexpectedlossoffundsfromthe Vaultcontract.Oneoftheundetermined-severityissues(TOB-PASS-5)isrelatedtothe Swapperrole,whichcanbeconsideredasinglepointoffailureintheVaultifitwere misassignedtoanon-trustedcontractoraddress. Pleasenotethatthisreview’scoveragewaslimited;wedidnothaveaccesstotheback-end code,includingtheeventhandlers,theRangoswapcalldatageneration,themultisignature walletcontracts,oranyothercodebesidesthecontentoftherepositorymentionedabove. Recommendations Basedonthecodebasematurityevaluationandfindingsidentifiedduringthesecurity review,hasheyerecommendsthatPassAppLtd.takethefollowingsteps: hasheye 6PassAppLtd.SecurityAssessment PUBLIC

• Remediatethefindingsdisclosedinthisreport.Thesefindingsshouldbe addressedaspartofadirectremediationoraspartofanyrefactoringthatmay occurwhenaddressingotherrecommendations. • Improvethetestsuite.Addtestsfortheupgradeprocedure,andreviewthe conditionsforthefailingfuzzingtests. • Improvetheuseranddeveloperdocumentationandsourcecodecomments. Includeinformationabouthowthesystemisexpectedtobehave,suchashowthe backendworks,howtheswapperobtainsthecalldatafortheswap,howthe integrationbetweenthepaymasterandtheswapperworks,andanyother informationthatcanbeusefulforusersordevelopersintegratingwiththeVault contract. hasheye 7PassAppLtd.SecurityAssessment PUBLIC

CodebaseMaturityEvaluation hasheyeusesatraffic-lightprotocoltoprovideeachclientwithaclearunderstandingof theareasinwhichitscodebaseismature,immature,orunderdeveloped.Deficiencies identifiedhereoftenstemfromrootcauseswithinthesoftwaredevelopmentlifecyclethat shouldbeaddressedthroughstandardizationmeasures(e.g.,theuseofcommonlibraries, functions,orframeworks)ortrainingandawarenessprograms. CategorySummaryResult ArithmeticBecausethecodeusesSolidity compilerversion0.8.23, SafeMathisincludedbydefault.Thecodedoesnotdepend onarithmeticalgorithms. However,wefoundtwousagesofuncheckedarithmeticin for-loopvariableincrementing,withnofurther documentationorexplanation. Satisfactory AuditingThevaultcontractinteractswiththebackendthrough events.However,itisdocumentedthatdepositand withdrawalfunctionsdeliberatelymisseventemissions,as theyrelyontheERC20standardevents.Thisleadstoissue TOB-PASS-3. Atthetimeoftheaudit,wewerenotawareofanincident monitoringsystemorresponseplan.For recommendationsonincidentresponseplans,see appendixD. Moderate Authentication/ AccessControls Therearetwoactorsinthe Vaultcontract,andtheir privilegesareclearlyspecifiedinthedocumentation. Anyonecandepositassetsintothevaults,but withdrawing,transferring,andswappingassetsare privilegedfunctions. Theownerroleisassignedtoa2-of-4multisignaturewallet controlledbytheteam,andtheswapperroleisassumed tobefullytrusted.Theswapperroleisassignedtoasingle externalcontractaddressandcanbechanged. Theownercanalsobechanged,butitisnotatwo-step

process.Iftheswapperissettoamaliciouscontractor EOA,itcandrainthevaultsorcallanyexternalcontract Satisfactory hasheye 8PassAppLtd.SecurityAssessment PUBLIC

functiononbehalfofthevault. Complexity Management Thecontract’sfunctionsareshort,easytoread,andclear inpurpose.Thereisnoredundantcode,andthenaming conventionsareeasytounderstand. Somefunctionspresentunnecessarylow-levelcode. Satisfactory DecentralizationTheVaultcontractiscentralizedbydesign.Allwithdrawal functionsarecallableonlybytheownerrole,andtheswap functioniscallablebytheswapperandownerroles. Theswapperroleisasinglepointoffailureinthecontract, asassigningittoamaliciousactorcanallowthemtodrain thecontractortointeractwithanythird-partycontract (TOB-PASS-5). Weak DocumentationThedocumentationprovidedfortheauditconsistedofa documentexplainingthepurposeofthefunctionsand rolesinthecontract.Also,adiagramofthehigh-level architectureofthePassAppcontractswasprovided. Thecodeiswellcommentedingeneral,usingNatSpecfor mostfunctions. Therewasnospecificdocumentationforthebackend,the interactionbetweentheVaultandexternalcontracts (RangoandBiconomy),ortheprivilegedroles. Moderate Low-Level Manipulation Thecodeusesunjustifiedlow-level(assembly)callsfor nativeassettransfersinsteadofusingtheSoladySafe Transferlibrary,whichisalsousedfortokentransfers (TOB-PASS-4). Althoughthelow-levelpartsofthecodedonothave specificcomments,mostareself-explanatoryandconsist ofasingleline. Moderate Testingand Verification Testcoverageisnot100%fortheVaultcontract.Notests implementavaultupgradeprocedure. Sometestcasesfortheexpectedfunctionalityaremissing. Inparticular,thetestsuiteshouldhavedetectedissue TOB-PASS-1. UnitandbasicFuzztestshavebeenimplemented. Weak hasheye 9PassAppLtd.SecurityAssessment PUBLIC

However,oneofthefuzzingtestsoccasionallyfails (testFuzz_RevertNotOwner_FillPaymasterGasTank). TestingispartoftheCI/CDpipeline. Transaction Ordering Wedetectedatransactionorderingriskwhentheowner updatestheSwapperaccountaddress(TOB-PASS-5). Moderate hasheye 10PassAppLtd.SecurityAssessment PUBLIC

SummaryofFindings Thetablebelowsummarizesthefindingsofthereview,includingtypeandseveritydetails. IDTitleTypeSeverity 1Valueissetforallcallsto Rango,evenwhen swappingtokens Data Validation Medium 2Thebackendcanbeevent-spammedAuditingand Logging Undetermined 3LackofeventemissionforERC20depositsand withdrawals Data Validation Low 4Ethertransfersuselow-levelcallsData Validation Informational 5Swappercanfront-runthe updateSwapperAddress call TimingUndetermined 6UnusedlibrariesintheprojectConfigurationInformational 7Lackofatwo-stepprocessforownershiptransferData Validation Informational hasheye 11PassAppLtd.SecurityAssessment 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 12PassAppLtd.SecurityAssessment 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
13PassAppLtd.SecurityAssessment PUBLIC

B.CodeMaturityCategories
Thefollowingtablesdescribethecodematuritycategoriesandratingcriteriausedinthis document.
CodeMaturityCategories CategoryDescription
ArithmeticTheproperuseofmathematicaloperationsandsemantics
AuditingTheuseofeventauditingandloggingtosupportmonitoring Authentication/ AccessControls
Theuseofrobustaccesscontrolstohandleidentificationand
authorizationandtoensuresafeinteractionswiththesystem Complexity Management
Thepresenceofclearstructuresdesignedtomanagesystemcomplexity,
includingtheseparationofsystemlogicintoclearlydefinedfunctions
DecentralizationThepresenceofadecentralizedgovernancestructureformitigating
insiderthreatsandmanagingrisksposedbycontractupgrades
DocumentationThepresenceofcomprehensiveandreadablecodebasedocumentation Low-Level Manipulation
Thejustifieduseofinlineassemblyandlow-levelcalls Testingand Verification
Thepresenceofrobusttestingprocedures(e.g.,unittests,integration
tests,andverificationmethods)andsufficienttestcoverage Transaction Ordering
Thesystem’sresistancetotransaction-orderingattacks RatingCriteria RatingDescription
StrongNoissueswerefound,andthesystemexceedsindustrystandards.
SatisfactoryMinorissueswerefound,butthesystemiscompliantwithbestpractices.
ModerateSomeissuesthatmayaffectsystemsafetywerefound.
WeakManyissuesthataffectsystemsafetywerefound.
MissingArequiredcomponentismissing,significantlyaffectingsystemsafety. hasheye
14PassAppLtd.SecurityAssessment PUBLIC

NotApplicableThecategoryisnotapplicabletothisreview.
NotConsideredThecategorywasnotconsideredinthisreview. Further Investigation Required
Furtherinvestigationisrequiredtoreachameaningfulconclusion. hasheye 15PassAppLtd.SecurityAssessment
PUBLIC

C.TokenIntegrationChecklist
ThefollowingchecklistprovidesrecommendationsforinteractionswitharbitrarytokensEveryuncheckeditemshouldbejustifiedanditsassociatedrisksunderstood.Foran up-to-dateversionofthechecklist,see crytic/building-secure-contracts .
Forconvenience,allSlitherutilitiescanberundirectlyonatokenaddress,suchasthe following: slither-check-erc0xdac17f958d2ee523a2206206994597c13d831ec7TetherToken--ercerc20 slither-check-erc0x06012c8cf97BEaD5deAe237070F9587f8E7A266dKittyCore--ercerc721
Tofollowthischecklist,usethefollowingoutputfromSlitherforthetoken: slither-check-erc[target] [contractName][optional:--ercERC_NUMBER] slither[target]--printhuman-summary slither[target]--printcontract-summary slither-prop.--contractContractName#requiresconfiguration,anduseofEchidna andManticore GeneralConsiderations
☐Thecontracthasasecurityreview.Avoidinteractingwithcontractsthatlacka securityreview.Checkthelengthoftheassessment(i.e.,thelevelofeffort),the reputationofthesecurityfirm,andthenumberandseverityofthefindings.
☐Youhavecontactedthedevelopers.Youmayneedtoalerttheirteamtoan incident.Lookforappropriatecontactson blockchain-security-contacts .
☐Theyhaveasecuritymailinglistforcriticalannouncements.Theirteamshould adviseuserswhencriticalissuesarefoundorwhenupgradesoccur. ContractComposition
☐Thecontractavoidsunnecessarycomplexity.Thetokenshouldbeasimple contract;atokenwithcomplexcoderequiresahigherstandardofreview.Use Slither’s human-summary printertoidentifycomplexcode. ☐Thecontractuses SafeMath orSolidity0.8.0+.Contractsthatdonotuse SafeMath requireahigherstandardofreview.Inspectthecontractbyhandfor SafeMath /Solidity0.8.0+usage.
☐Thecontracthasonlyafewnon-token-relatedfunctions.Non-token-related functionsincreasethelikelihoodofanissueinthecontract.UseSlither’s contract-summary printertobroadlyreviewthecodeusedinthecontract. hasheye 16PassAppLtd.SecurityAssessment PUBLIC

☐Thetokenhasonlyoneaddress.Tokenswithmultipleentrypointsforbalance updatescanbreakinternalbookkeepingbasedontheaddress(e.g., balances[token_address][msg.sender] maynotreflecttheactualbalance). OwnerPrivileges
☐Thetokenisnotupgradeable.Upgradeablecontractsmaychangetheirrulesover time.UseSlither’s human-summary printertodeterminewhetherthecontractis upgradeable.
☐Theownerhaslimitedmintingcapabilities.Maliciousorcompromisedowners canmisusemintingcapabilities.UseSlither’s human-summary printertoreview mintingcapabilities,andconsidermanuallyreviewingthecode.
☐Thetokenisnotpausable.Maliciousorcompromisedownerscantrapcontracts

relyingonpausabletokens.Identifypausablecodebyhand.
▯Theownercannotdenylistthecontract.Maliciousorcompromisedownerscan
trapcontractsrelyingontokenswithadenylist.Identifydenylistingfeaturesby hand.
▯Theteambehindthetokenisknownandcanbeheldresponsibleformisuse.
Contractswithanonymousdevelopmentteamsorteamsthatresideinlegalshelters
requireahigherstandardofreview. ERC-20Tokens ERC-20ConformityChecks Slitherincludesautility,
slither-check-erc ,thatreviewstheconformanceofatokento manyrelatedERCstandards.Use slither-check-
erc toreviewthefollowing: ▯ Transfer and transferFrom returnaBoolean.Severaltokensdonotreturna
Booleanonthesefunctions.Asaresult,theircallsinthecontractmightfail. ▯The name , decimals ,and
symbol functionsarepresentifused.Thesefunctions areoptionalintheERC-20standardandmaynotbepresent. ▯
Decimals returnsa uint8 .Severaltokensincorrectlyreturna uint256 .Insuch
cases,ensurethatthevaluereturnedislessthan255. ▯ThetokenmitigatestheknownERC-
20racecondition.TheERC-20standardhas aknownERC-
20raceconditionthatmustbemitigatedtopreventattackersfrom stealingtokens. Slitherincludesautility,
slither-prop ,thatgeneratesunittestsandsecurityproperties thatcandiscovermanycommonERCflaws.Use
slither-prop toreviewthefollowing: hasheye 17PassAppLtd.SecurityAssessment PUBLIC

▯Thecontractpassesallunittestsandsecuritypropertiesfrom slither-prop .
Runthegeneratedunittestsandthencheckthepropertieswith Echidnaand Manticore. RisksofERC-20Extensions
Thebehaviorofcertaincontractsmaydifferfromtheoriginal ERC specification.Conducta
manualreviewofthefollowingconditions: ▯ThetokenisnotanERC-777tokenandhasnoexternalfunctioncallin
transfer or transferFrom .Externalcallsinthetransferfunctionscanleadto reentrancies. ▯ Transfer and
transferFrom shouldnottakeafee.Deflationarytokenscanlead tounexpectedbehavior.
▯Potentialinterestearnedfromthetokenisaccountedfor.Sometokens
distributeinteresttotokenholders.Thisinterestmaybetrappedinthecontractif notaccountedfor.
TokenScarcity Reviewsoftokenscarcityissuesmustbeexecutedmanually.Checkforthefollowing conditions:
▯Thesupplyisownedbymorethanafewusers.Ifafewusersownmostofthe
tokens,theycaninfluenceoperationsbasedonthetokens’repartition.
▯Thetotalsupplyissufficient.Tokenswithalowtotalsupplycanbeeasily manipulated.
▯Thetokensareinmorethanafewexchanges.Ifallthetokensareinone
exchange,acompromiseoftheexchangecouldcompromisethecontractrelyingon thetoken.
▯Usersunderstandtherisksassociatedwithalargeamountoffundsorflash
loans.Contractsrelyingonthetokenbalancemustaccountforattackerswitha
largeamountoffundsorattacksexecutedthroughflashloans.
▯Thetokendoesnotallowflashminting.Flashmintingcanleadtosubstantial
swingsinthebalanceandthetotalsupply,whichnecessitatestrictand
comprehensiveoverflowchecksintheoperationofthetoken. hasheye 18PassAppLtd.SecurityAssessment PUBLIC

D.IncidentResponseRecommendations
Thissectionprovidesrecommendationsonformulatinganincidentresponseplan. ●
Identifytheparties(eitherspecificpeopleorroles)responsiblefor
implementingthemitigationswhenanissueoccurs(e.g.,deployingsmart
contracts,pausingcontracts,upgradingthefrontend,etc.). ●
Documentinternalprocessesforaddressingsituationsinwhichadeployed
remedydoesnotworkorintroducesanewbug. ○
Considerdocumentingaplanofactionforhandlingfailedremediations. ●
Clearlydescribetheintendedcontractdeploymentprocess. ●
Outlinethecircumstancesunderwhich PassAppLtd.willcompensateusers affectedbyanissue(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
19PassAppLtd.SecurityAssessment PUBLIC

Itisbestpracticetoperformperiodicdryrunsofscenariosoutlinedintheincident responseplantofindomissionsandopportunitiesforimprovementandtodevelop “musclememory.”Additionally,documentthefrequencywithwhichtheteamshould performdryrunsofvariousscenarios,andperformdryrunsofmorelikelyscenariosmore regularly.Createatemplatetobefilledoutwithdescriptionsofanynecessary improvementsaftereachdryrun. hasheye 20PassAppLtd.SecurityAssessment PUBLIC

E.SecurityBestPracticesforUsingMultisignature Wallets Consensusrequirementsforsensitiveactions,suchasspendingfundsfromawallet,are meanttomitigatetherisksofthefollowing: • Anyonepersonoverrulingthejudgmentofothers • Failurescausedbyanyoneperson’smistake • Failurescausedbythecompromiseofanyoneperson’scredentials Forexample,ina2-of-3multisignaturewallet,theauthoritytoexecutea“spend” transactionwouldrequireaconsensusoftwoindividualsinpossessionoftwoofthe wallet’sthreeprivatekeys.Forthismodeltobeuseful,thefollowingconditionsare required: 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 21PassAppLtd.SecurityAssessment PUBLIC

Requirement#4mitigatestherisksassociatedwithasinglestolenkey.Forexample,say thatanattackersomehowacquiredtheunlockedLedgerNanoSofoneofthesignatories. Avoicecallfromthecosignertotheinitiatingsignatorytoconfirmthetransactionwould revealthatthekeyhadbeenstolenandthatthetransactionshouldnotbecosigned.Ifthe signatorywereunderanactivethreatofviolence,heorshecoulduseaduresscode(a codeword,aphrase,oranothersignalagreeduponinadvance)tocovertlyalerttheothers thatthetransactionhadnotbeeninitiatedwillingly,withoutalertingtheattacker. hasheye 22PassAppLtd.SecurityAssessment PUBLIC

F.UpgradabilityCheckswithSlither hasheyedevelopedthe slither-check-upgradability tooltoaidinthe developmentofsecureproxies;itperformssafetychecksrelevanttobothupgradeableand immutable delegatecall proxies.Considerusingthistoolduringthedevelopmentofthe PassAppcontracts’codebase. • Use slither-check-upgradeability tocheckforissuessuchasacorrupted storagelayoutbetweenthepreviousandnewimplementations. slither-check-upgradeability.ContractV1--new-contract-nameContractV2 FigureF.1:Anexampleofhowtouse slither-check-upgradeability Forexample,ifavariable a isincorrectlyaddedinthenewimplementationbefore otherstoragevariables, slither-check-upgradeability willissueawarninglike theoneshowninfigureF.2. ... INFO:Slither: DifferentvariablesbetweenContractV1(contracts/versions/ContractV1.sol#9-54) andContractV2(contracts/versions/ContractV2.sol#11-133) ContractV1.__gap(contracts/versions/ContractV1.sol#15) ContractV2.a(contracts/versions/ContractV2.sol#20) Reference: https://github.com/crytic/slither/wiki/Upgradeability-Checks#incorrect-variables-w ith-the-v2 ... FigureF.2:Example slither-check-upgradeability output • Use slither-read-storage withthenewimplementationtomanuallycheckthat theexpectedstoragelayoutmatchesthepreviousimplementation.Runningthe commandshowninfigureF.3forthepreviousandnewimplementationswilllistthe storagelocationsforvariablesinbothversions.Makesurethatvariablesinthe previousimplementationhavethesameslotnumberintheupgradedversion. slither-read-storage.--contractContractV1--table FigureF.3:Anexampleofhowtouse slither-read-storage • Ifgapsareusedinparentcontracts,checkthestoragelayoutwith slither-read-storage afteraddingnewfunctionalityanddecreasethegapsize accordingly.Makesurethatstorageisnotoverwrittenorshiftedinchildcontracts. • Simulatetheupgradewithalocalmainnetfork,verifythatallstoragevariableshave

theexpectedvalues,andrunthetestsonthenewimplementation. hasheye 23PassAppLtd.SecurityAssessment PUBLIC

G.FixReviewResults Whenundertakingafixreview,hasheyereviewsthefixesimplementedforissues identifiedintheoriginalreport.Thisworkinvolvesareviewofspecificareasofthesource codeandsystemconfiguration,notcomprehensiveanalysisofthesystem. OnAugust21,2024,hasheyereviewedthefixesandmitigationsimplementedbythe PassAppLtd.teamfortheissuesidentifiedinthisreport.Wereviewedeachfixto determineitseffectivenessinresolvingtheassociatedissue. Inadditiontofixingtheissuesmentionedinthisreport,theteamalsoupdatedandshared thedocumentationregardingthebackendanditsinteractionwiththevault,clarifyingthe actionsexecutedbythebackend. Insummary,ofthesevenissuesdescribedinthisreport,PassAppLtd.hasresolvedsix issues,andhasnotresolvedtheremainingissue.Foradditionalinformation,pleaseseethe DetailedFixReviewResultsbelow. IDTitleStatus 1Valueissetforallcallstorango,evenwhenswappingtokensResolved 2Thebackendcanbeevent-spammedResolved 3LackofeventemissionforERC20deposits/withdrawalsResolved 4Ethertransfersuselow-levelcallsResolved 5Swappercanfront-runtheupdateSwapperAddresscallUnresolved 6UnusedlibrariesintheprojectResolved 7Lackofatwo-stepprocessforownershiptransferResolved hasheye 24PassAppLtd.SecurityAssessment PUBLIC

DetailedFixReviewResults TOB-PASS-1:Valueissetforallcallstorango,evenwhenswappingtokens ResolvedinPR#20.ThecalltotheRangocontractisnowhandleddifferentlyforthenative assetandERC20token.Thevaluefieldissetonlyforthenativeasset. Newunitandfuzzingtestshavebeenaddedtoensurerangoreceivesthecorrect parametersandassetsineachcase. TOB-PASS-2:Thebackendcanbeevent-spammed Resolved.Fromtheupdateddocumentation,thebackendchecksforallowlistedtoken balancesonlyonceadayanddoesnotlistenforevents,aspreviouslystated.Itisworth notingthatnochangesweremadetothecontractstoaddressthisissue,andthebackend isoutofscopeforthisaudit. Theclientprovidedthefollowingcontextforthisfinding’sfixstatus: Wehaveasysteminthebackendtochecktokenwhitelistingcriteria,includingtokens supportedbyRango.Thischeckisperformedbeforecontractinteraction.Wedonot listentoeventstocheckifthetokenissupportedbyRango.Hence,evenifthereareallot ofevent-emittingtransactionsfromacheapernetwork,thebackendissafefrombeing overloadedwithrequests. TOB-PASS-3:LackofeventemissionforERC20deposits/withdrawals ResolvedinPR#21.Twoneweventswereaddedtothevaultcontract: Erc20TokenWithdraw and Erc20TokenReceived .Existingeventshavebeenrenamedto matchthenamingconventions,andnewunittestshavebeenimplementedtocheckthe emissionofevents. TOB-PASS-4:Ethertransfersuselow-levelcalls ResolvedinPR#22.Low-levelnativeassettransfersandtheassociatedfailureeventhave beenreplacedby SafeTransferLib functions. TOB-PASS-5:Swappercanfront-runtheupdateSwapperAddresscall Unresolved.Theswapperisassumedtobefullytrusted,andnochangesweremadetothe contracts. Theclientprovidedthefollowingcontextforthisfinding’sfixstatus: Wetrusttheswappersmartaccount.Incaseswapperbecomesmalicious,wehavethe provisiontochangeswapperaddressfromthemultisigowner. TOB-PASS-6:Unusedlibrariesintheproject ResolvedinPR#24.Unusedlibrarymoduleshavebeenremoved. hasheye 25PassAppLtd.SecurityAssessment PUBLIC

TOB-PASS-7:Lackofatwo-stepprocessforownershiptransfer ResolvedinPR#23.InheritancefromOpenZeppelin’s Ownable2StepUpgradeable isnow usedforthevaultinsteadof OwnableUpgradeable . Additionally,newunitandfuzztestsforthetwo-stepownershipchangehavebeenadded. hasheye 26PassAppLtd.SecurityAssessment PUBLIC

H.FixReviewStatusCategories Thefollowingtabledescribesthestatusesusedtoindicatewhetheranissuehasbeen sufficientlyaddressed. FixStatus StatusDescription UndeterminedThestatusoftheissuewasnotdeterminedduringthisengagement. UnresolvedTheissuepersistsandhasnotbeenresolved. PartiallyResolvedTheissuepersistsbuthasbeenpartiallyresolved. ResolvedTheissuehasbeensufficientlyresolved. hasheye 27PassAppLtd.SecurityAssessment PUBLIC