HashEye

// SMART CONTRACT SECURITY AUDIT

Arcade

Security assessment by HashEye · prepared for Arcade

HASHEYE AUDITED

PROJECT	Arcade
CLIENT	Arcade
CATEGORY	Blockchain
PUBLISHED	July 1, 2023
REPORT ID	research-arcade-2023-07-01-lsnflv

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-arcade-2023-07-01-lsnflv.

Arcade.xyzV3 SecurityAssessment July31,2023 Preparedfor: CaryGalant Arcade.xyz Preparedby:AlexanderRemie,GuillermoLarregay,andRobertSchneider

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. 228ParkAveS#80688 NewYork,NY10003 https://www.hasheye.io info@hasheye.io hasheye 1Arcade.xyzV3SecurityAssessment PUBLIC

NoticesandRemarks CopyrightandDistribution Thisreportisconsideredbyhasheyetobepublicinformation;itislicensedtoArcade.xyz underthetermsoftheprojectstatementofworkandhasbeenmadepublicatArcade.xyz's request.Materialwithinthisreportmaynotbereproducedordistributedinpartorin wholewithouttheexpresswrittenpermissionofhasheye. ThesolecanonicalsourceforhasheyepublicationsisthehasheyePublicationspage. Reportsaccessedthroughanysourceotherthanthatpagemayhavebeenmodifiedand shouldnotbeconsideredauthentic. TestCoverageDisclaimer Allactivitiesundertakenbyhasheyeinassociationwiththisprojectwereperformedin accordancewithastatementofworkandagreeduponprojectplan. Securityassessmentprojectsaretime-boxedandoftenreliantoninformationthatmaybe providedbyaclient,itsaffiliates,oritspartners.Asaresult,thefindingsdocumentedin thisreportshouldnotbeconsideredacomprehensivelistofsecurityissues,flaws,or defectsinthetargetsystemorcodebase. hasheyeusesautomatedtestingtechniquestorapidlytestthecontrolsandsecurity propertiesofsoftware.Thesetechniquesaugmentourmanualsecurityreviewwork,but eachhasitslimitations:forexample,atoolmaynotgeneratearandomedgecasethat violatesapropertyormaynotfullycompleteitsanalysisduringtheallottedtime.Theiruse isalsolimitedbythetimeandresourceconstraintsofaproject. hasheye 2Arcade.xyzV3SecurityAssessment PUBLIC

TableofContents

15.Thefeevaluescandistorttheincentivesfortheborrowersandlenders53
16.MaliciousborrowerscanuseforceRepaytogrieflenders54 A.VulnerabilityCategories56
B.CodeMaturityCategories58 C.CodeQualityRecommendations60
D.RiskswithApprovingNFTsforUseasCollateral62 hasheye 3Arcade.xyzV3SecurityAssessment PUBLIC

E.TokenIntegrationChecklist65 F.MutationTesting70 G.IncidentResponsePlanRecommendations73
H.FixReviewResults75 DetailedFixReviewResults76 hasheye 4Arcade.xyzV3SecurityAssessment PUBLIC

ExecutiveSummary EngagementOverview
ArcadeengagedhasheyetoreviewthesecurityoftheArcade.xyzV3protocol.The
protocolisanNFTlendingplatformthatallowsuserstoinitiate,rollover,andrepayloans,
withuniqueNFTsandotherassetsservingascollateraltobackloans.Itimplementsa
networkofcontractstohandleloanmanagement,feeassessment,andassetvaulting,
whicheffectivelyallowsuserstobundleassetsintoasingletransferableNFTthatcanbe usedascollateral.
AteamofthreeconsultantsconductedthereviewfromMay15toJune9,2023,foratotal ofeightengineer-
weeksofeffort.Ourtestingeffortsfocusedonthesecurity,reliability,and
functionalityoftheprotocol.Withfullaccesstothesourcecodeanddocumentation,we
performedstaticanddynamictestingoftheprotocol,usingautomatedandmanual processes.
ObservationsandImpact Arcade’sNFTlendingprotocolusesadequateaccesscontrolsandisprotectedagainst
potentialattackvectorssuchasreentrancyandfront-running.Nonetheless,weidentified
consistentissuesacrossvariouscomponents,particularlythoserelatedtoinputvalidation,
returnvaluechecks,andpotentiallossofaccesstofunds(TOB-ARCADE-8, TOB-ARCADE-
12),indicatinganeedforenhanceddatavaliditychecksandsafeguarding
mechanisms.Concernsregardingtheapprovalmechanism(TOB-ARCADE-3)andevent emissions(TOB-ARCADE-1,TOB-
ARCADE-4)indicateaneedformorerobustloggingand ERC-
20tokenmanagement.Furthermore,weidentifiedissuesrelatedtoincorrect implementationsandoperations—
liketheincorrectencodingofthe itemPredicates parameter,whichobfuscatestheverifieraddress(TOB-
ARCADE-14),andmisaligned incentivesforadheringtotheexpectedorderofoperations(TOB-ARCADE-
16);theseissues suggestthatfurtherattentionisneededtorefinecertainimplementationsandprevent
invalidorexploitableoperations.Althoughcriticalsecuritymeasuresareimplementedin
theprotocol,improvementsarenecessaryintheareasofdatavalidation,logging,timing, andconfiguration.
Recommendations Basedonthecodebasematurityevaluationandfindingsidentifiedduringthesecurity
review,hasheyerecommendsthattheArcadeteamtakethefollowingsteps: ●
Remediatethefindingsdisclosedinthisreport.Thesefindingsshouldbe
addressedaspartofadirectremediationoraspartofanyrefactorthatmayoccur
whenaddressingotherrecommendations. hasheye 5Arcade.xyzV3SecurityAssessment PUBLIC

● Ensurethatallinputsandexpectedreturnvaluesarevalidated (TOB-ARCADE-5andTOB-ARCADE-
8).Wefoundissuesrelatedtoinputandreturn valuevalidationinseveralcontracts,including LoanCore ,
OriginationController , RepaymentController , VaultFactory ,and AssetVault
.Theseissuessuggestthatthevalidityofinputdataandresponses
fromthecontractfunctionsmightnotbeadequatelyenforcedorverifiedacrossthe protocol. ●
Developanincidentresponseplan.SuchaplanwillhelptheArcadeteamto
prepareforfailurescenariosandwilloutlinetheappropriateresponsestothem.
RefertoappendixGforguidanceoncreatinganincidentresponseplan. ● Updatetheuser-
facingdocumentationtoreflectV3oftheprotocol.The currentdocumentationisrelatedtoV2oftheprotocol.Up-
to-dateuser-facing documentationwilllimittheriskofuserconfusionduetochangesbetweenV3and V2. ●
Improvetheinlinecomments.Somepartsoftheimplementation(suchasthe rollovermechanismandthe
PunksVerifier contract)aredifficulttounderstand
duetoinsufficientcommentstoexplaintheimplementation. ●
Improvetheunittestingsuite.Althoughtestcoverageisat100%,theunittesting
suitestillhasgaps,whichhascausedissueslikeTOB-ARCADE-5andTOB-ARCADE-9 topersistunnoticed.
BreakdownofFindings Thefollowingtablesprovidethenumberoffindingsbyseverityandcategory. hasheye
6Arcade.xyzV3SecurityAssessment PUBLIC

EXPOSUREANALYSIS SeverityCount High0 Medium4 Low5 Informational6 Undetermined1 CATEGORYBREAKDOWN
CategoryCount AccessControls1 Configuration1 DataValidation6 ErrorReporting1 Testing1 Timing2
UndefinedBehavior4 hasheye 7Arcade.xyzV3SecurityAssessment PUBLIC

ProjectSummary ContactInformation Thefollowingmanagerswereassociatedwiththisproject:
DanGuido,AccountManagerSamGreenup,ProjectManager dan@hasheye.iosam.greenup@hasheye.io
Thefollowingengineerswereassociatedwiththisproject:
AlexanderRemie,ConsultantGuillermoLarregay,Consultant
alexander.remie@hasheye.ioguillermo.larregay@hasheye.io RobertSchneider,Consultant
robert.schneider@hasheye.io ProjectTimeline
Thesignificanteventsandmilestonesoftheprojectarelistedbelow. DateEvent May11,2023Pre-
projectkickoffcall May22,2023Statusupdatemeeting#1 May30,2023Statusupdatemeeting#2

June5,2023Statusupdatemeeting#3 June12,2023Deliveryofreportdraftandreportreadoutmeeting July31,2023Deliveryoffinalreportwithfixreview hasheye 8Arcade.xyzV3SecurityAssessment PUBLIC

ProjectGoals Theengagementwasscopedtoprovideasecurityassessmentoftheˆ Arcade.xyzV3NFT lendingprotocol.Specifically,wesoughttoanswerthefollowingnon-exhaustivelistof questions: • DotheNFTsusedintheprotocolcomplywithstandardinterfaceslikeERC-721, ERC-1155,andERC-20? DotheNFTsdeviatefromthesestandardsinawaythat couldintroduceunexpectedbehaviorsorcompatibilityissues?Arethe“safe” versionsofthefunctionsofthesestandardsused? • Istheprotocol'sclaimprocess(whichistriggeredwhenaborrowerfailstorepaya loan)fair,transparent,andsecure,preventingunfairliquidationofNFTs? • Doestheprotocolimplementmeasurestopreventfront-running,especiallyfor sensitiveoperationslikeloanrepaymentandliquidation? • Aretheassetvaultsimplementedsecurely,protectingborrowers’fundsandtheir accesstothematalltimes? Additionally,doestheuseofassetvaultsinanyway preventlendersfrombeingabletoclaimcollateralwhentheirloansarenotrepaid? • Doesthesystemhandleloaninitializationandrepaymentsproperly,includingthose involvingmultipleassetsandvarioustypesofNFTs? • Doestheprotocolensurethatthe tokenURI foreachNFT,whichpointstoits metadata,isimmutableafterminting,preventingamalicioususerfromchangingit? • Aretherulesandparameterssurroundingcollateralrequirementsinthelending protocolclearlydefinedandsecure,providingadequatesafeguardsincaseof attemptedfraud? • DoestheprotocolcorrectlyandsecurelyimplementEIP-712forstructureddata hashingandsigning? Arethererobustmeasuresinplacetopreventpotential securityissuesrelatedtothemisuseofdomainseparatorsortypehashes? • Arerole-basedaccesscontrolssecurelyandeffectivelyimplementedwithinthe system? Aretheresafeguardspreventingunauthorizedaccess,andaretheroles appropriatelyassignedtopreventpotentialexploitationormisuse? hasheye 9Arcade.xyzV3SecurityAssessment PUBLIC

ProjectTargets Theengagementinvolvedareviewandtestingofthefollowingtarget. Arcade.xyz Repositoryhttps://github.com/arcadexyz/arcade-protocol Version 4f510e0e2287901abb21265f72aa4465166ab09d TypeSolidity PlatformEthereum hasheye 10Arcade.xyzV3SecurityAssessment PUBLIC

ProjectCoverage Thissectionprovidesanoverviewoftheanalysiscoverageofthereview,asdeterminedby ourhigh-levelengagementgoals.Ourapproachesincludedthefollowing: Core • LoanCore :The LoanCore contractisthecorecontractoftheprotocol.Bothofthe controllercontractscallfunctionsinthiscontract.Thiscontractcontainsfunctionsto startloans,repayloans,claimthecollateralbackingloansthathavenotbeen repaid,rolloverloans,andwithdrawfees.Wereviewedtheimplementationfor vulnerabilitiesthatcouldallowattackerstostealfundsorcauseadenialofservice, andwelookedforwaysthatuserscouldloseaccesstotheirfunds(TOB-ARCADE-8). Additionally,wereviewedtheaccesscontrols,eventemission,inputvalidation,and pausingmechanismofthecontract.Wealsocloselyreviewedthecorrectnessofthe rollovermechanismandstatemachineandlookedforopportunitiestoperform reentrancyandfront-runningattacks.Lastly,wereviewedthecontracttoensure thatitcorrectlyappliesfees,usespromissorynotescorrectly,andsafelytransfers ERC-20,ERC-721,andERC-1155tokens. • OriginationController :Thisisoneofthetwomaincontrollercontractsthrough whichusersinteractwiththeprotocol.Thiscontractperformsvalidationsoncalls madeto LoanCore ,whichperformstheactualoperations.Thiscontractcontains functionstostartloansandtorolloverloans.Wereviewedtheimplementationto lookforflawsrelatedtoinputvalidation,accesscontrols,missingevents,loopsthat exhaustgas,signatureverificationvulnerabilities,EIP-712adherence,ERC-2612 (permit)adherence,andfront-runningandreentrancyvulnerabilities.Additionally, welookedforwaystocreateloanswithinvalidterms,createloanswithinvalid counterparties,rolloverloanswithoutfullyrepayingthepreviousloans,orsubvert therollovermechanisminotherways. • RepaymentController :Thisisthesecondofthetwomaincontrollercontracts throughwhichusersinteractwiththeprotocol.Thiscontractperformsvalidations oncallsmadeto LoanCore ,whichperformstheactualoperations.Thiscontract containsfunctionstorepayloansandtoclaimthecollateralbackingloansthat endedbutwerenotrepaid.Wereviewedtheaccesscontrols,inputvalidation (TOB-ARCADE-8),andfeecalculations.Welookedforfront-runningandreentrancy vulnerabilities.Additionally,welookedforwaystorepayaloanwithoutactuallyfully repayingit,flawsinthewithdrawaloflenderfundsusingthe redeemNote function,

transactionorderingflawsbetweenrepaymentandliquidation(TOB-ARCADE-13), flawsthatcouldpreventborrowersfromfullyrealizingthevalueoftheirloans withoutriskingdefault(TOB-ARCADE-13),andwaysforattackerstoillegitimately claimborrowers’collateral. hasheye 11Arcade.xyzV3SecurityAssessment PUBLIC

• FeeController :Thiscontractcontainstheconfiguredfeesandfunctionstoupdate thefeevalues,adheringtothemaximumfeeamountperfeecategory.Wereviewed theimplementationforissuesrelatedtoaccesscontrols,inputvalidation,and missingconfigurationsofmaximumfees(TOB-ARCADE-9).Additionally,wereviewed theeffectofchangingconfiguredfeeswhileloansareactive(TOB-ARCADE-10). • PromissoryNote :ThiscontractimplementsanERC-721tokenthatisusedtotrack thelenderandborrowerpartiesinvolvedinaloan.ThisNFTismintedwhenaloan isstartedandburnedwhentheloanends(throughrepaymentortheclaimingof collateral).Wereviewedtheaccesscontrols,inputvalidation,andreturnvalue validation(TOB-ARCADE-5).Additionally,wereviewedtheimplementationof overriddenOpenZeppelinfunctionstoensurethatthecontractstilladherestothe ERC-721standard. Vaults • VaultFactory :Thiscontractcanbeusedbypotentialborrowerstodeployan AssetVault contractthroughaminimalproxypattern.The VaultFactory contractisbothafactoryandanERC-721token.Foreachdeployed AssetVault contract,anaccompanyingERC-721tokenisminted;theownerofthistokenisthe owneroftheassociated AssetVault contract.Wereviewedtheimplementationto lookforflawsrelatedtoaccesscontrols,reentrancy,eventemission,inputvalidation (TOB-ARCADE-8),andreturnvaluevalidation(TOB-ARCADE-5).Additionally,we reviewedtheclaimfeesfunctionforanyflawsthatmightpreventfeesfrombeing withdrawable(TOB-ARCADE-7),andwecheckedfortheuseof SafeERC20 functions whereverpossible(TOB-ARCADE-12). • AssetVault :Thiscontractcanbedeployedbyusersthroughthe VaultFactory contractandisusedtobundlemultipleassets(ERC-20,ERC-721,ERC-1155,ETH, CryptoPunks)insideoneNFT(the VaultFactory NFT—refertothebulletpoint above).ThisbundledNFTcanthenbeusedascollateraltobackloans.Wemanually reviewedthecontracttolookforflawsrelatedtoaccesscontrols,reentrancy, front-running,inputvalidation,initialization,ownershiptracking,andinconsistent errormessages.Wealsolookedforwaysthatattackerscouldstealfundsfroman assetvaultandthattheownerofanassetvaultcouldwithdrawitsassetswhileitis beingusedascollateralinanactiveloan.Additionally,weinvestigatedwhetherthe functionalityallowinguserstonestassetvaultscouldcauseanyproblems,suchas thelossofaccesstothefundswithinanassetvault(TOB-ARCADE-11).Lastly,we reviewedtheuseofsafetransferfunctionstowithdrawassets,theapproval mechanism(TOB-ARCADE-3),theaccesscontrolsandimplementationofthevarious “call”functions,andthemechanismfordisablingandenablingwithdrawals. • CallWhitelist , CallWhitelistApprovals , CallWhitelistDelegation ,and CallWhitelistAllExtensions :Thesefourcontractstogether(through hasheye 12Arcade.xyzV3SecurityAssessment PUBLIC

inheritance)makeupthe“whitelist”contractthatisattachedtodeployed AssetVault contractsandisusedtoallow/disallowspecificfunctionstobecalled fromthe AssetVault contract.Thisismostlyusedtobeabletoparticipatein airdropswhileanNFTislockedupinanassetvault.Theownerofthe“whitelist” contractisallowedtowhitelistfunctions;inpractice,theownerwillbean Arcade-ownedaccountoragovernancesystem.Wemanuallyreviewedthecontract forflawsrelatedtoinheritance,inputvalidation,accesscontrols,andeventemission (TOB-ARCADE-4).Additionally,wereviewedtheuseoftheblacklistandwhitelistto determinewhetherwhitelistedcallsthatarealsopresentintheblacklistwouldstill bedeemedwhitelisted. Verifiers • ItemsVerifier :Thiscontractverifiesthatassetvaultshaveanassetoralistof assets(ERC-20,ERC-721,ERC-1155).Wemanuallyreviewedthecontracttocheck thatthedescribedspecificationadherestotheimplementationandtolookforany edgecasesthatarenothandledcorrectly.Additionally,wereviewedthewildcard processtodeterminewhetheritcouldbesomehowusedbyanattacker. • CollectionWideOfferVerifier :ThiscontractchecksthattheNFTcollateralin theloantermsisequaltotheNFTspecifiedinthepredicate.Anytokenwithinan NFTcollectionwouldsatisfythisverifier—thecontractdoesnotcheckforaspecific tokenId withinanNFTcollection.Wemanuallyreviewedthecontracttocheckthat thedescribedspecificationadherestotheimplementationandthatallrequired validationispresent. • UnvaultedItemsVerifier :Thiscontractchecksthatthecollateraltokeninthe loantermsandits tokenId matchthosespecifiedinthepredicate.Wemanually reviewedthecontracttocheckthatthedescribedspecificationadherestothe implementationandthatallrequiredvalidationispresent. • PunksVerifier

:ThiscontractchecckswhetheraCryptoPunk(anyCryptoPunkora specificCryptoPunk)ispresentinthecollateralspecifiedintheloanterms.We manuallyreviewedthecontracttocheckthatthedescribedspecificationadheresto theimplementationandthatthevalidationiscorrect.Wealsoreviewedthe CryptoPunkscontracttoensurethattheintegrationisimplementedcorrectly. • ArtBlocksVerifier :ThiscontractchecckswhetheratokenwithinalistofsupportedArtBlockscollections(anyArtBlockstokenoraspecifictoken)ispresent inthecollateralspecifiedintheloanterms.Wemanuallyreviewedthecontracttocheckthatthedescribedspecificationadherestotheimplementationandthatthevalidationiscorrect.WealsoreviewedthesupportedArtBlockscontracttoensurethattheintegrationisimplementedcorrectly. hasheye 13Arcade.xyzV3SecurityAssessment PUBLIC

CoverageLimitations Becauseofthetime-boxednatureoftestingwork,itiscommontoencountercoverage limitations.Thefollowinglistoutlinesthecoveragelimitationsoftheengagementand indicatessystemelementsthatmaywarrantfurtherreview: • Decentralizedgovernance:TheArcadeprotocolusesadecentralizedgovernance systemconsistingofmultiplesmartcontracts.Thesecontractswerenotpartofthe repositoryunderreviewandwereconsideredoutofscope.Werecommend performingaseparateaudittoreviewthegovernance-relatedsmartcontracts. • ExternalcontractsforunittestsTheprovidedrepositorycontainsvarioushelper contractsthatareusedonlytowriteunitteststhatinteractwiththeseexternal contracts.Forexample,theseexternalcontractsincludeanimplementationofthe EIP-5639standardandacopyoftheCryptoPunkssmartcontract.Thesecontracts wereallconsideredoutofscopeandmaywarrantaseparatereview. • OpenZeppelinlibraries:TheArcadeprotocolusestheOpenZeppelin-provided smartcontracts(version4.3.2).Thesecontractswereconsideredoutofscopefor thisaudit. • Frontend:TheArcadesystemalsoincludesafrontendtointeractwiththesmart contracts.Thefrontendwasconsideredoutofscopeforthisauditandmaywarrant aseparatereview. hasheye 14Arcade.xyzV3SecurityAssessment PUBLIC

AutomatedTesting hasheyeusesautomatedtechniquestoextensivelytestthesecuritypropertiesof software.Weusebothopen-sourcestaticanalysisandfuzzingutilities,alongwithtools developedinhouse,toperformautomatedtestingofsourcecodeandcompiledsoftware. TestHarnessConfiguration Weusedthefollowingtoolsintheautomatedtestingphaseofthisproject: ToolDescriptionPolicy UniversalmutatorAdeterministicmutationgeneratorthatdetects gapsintestcoverage AppendixF TestResults Theresultsofthisfocusedtestingaredetailedbelow. Universalmutator:Thefollowingtabledisplaystheproportionofmutantsforwhichall unittestspassed.Asmallnumberofvalidmutantsindicatesthattestcoverageisthorough andthatanynewlyintroducedbugsarelikelytobecaughtbythetestsuite.Alargenumber ofvalidmutantsindicatesgapsinthetestcoveragewhereerrorsmaygounnoticed.We usedtheresultsinthefollowingtabletoguideourmanualreview,givingextraattentionto codeforwhichtestcoverageappearstobeincomplete. Itisimportanttonotethatsomeofthevalidmutantscanbefalsepositives,suchas mutantsthatremovethepublicvisibilitymodifierfromapublicfunctionorvariable.These resultsmustbemanuallycheckedbeforedrawingconclusions.RefertoappendixFfor moreinformation. TargetValidMutants contracts/FeeController.sol 5.88% contracts/LoanCore.sol 8.68% contracts/OriginationController.sol 5.65% contracts/PromissoryNote.sol 13.65% hasheye 15Arcade.xyzV3SecurityAssessment PUBLIC

contracts/RepaymentController.sol 5.97% contracts/libraries/FeeLookups.sol 23.21% contracts/libraries/InterestCalculator.sol 13.33% contracts/libraries/LoanLibrary.sol 12.20% contracts/errors/Lending.sol 3.07% contracts/errors/Vault.sol 2.35% contracts/vault/AssetVault.sol 8.10% contracts/vault/CallBlacklist.sol 5.70% contracts/vault/CallWhitelist.sol 6.25% contracts/vault/CallWhitelistAllExtensions.sol 8.33% contracts/vault/CallWhitelistApprovals.sol 8.86% contracts/vault/CallWhitelistDelegation.sol 9.09% contracts/vault/OwnableERC721.sol 4.69% contracts/vault/VaultFactory.sol 11.35% contracts/verifiers/ArtBlocksVerifier.sol 0.0% contracts/verifiers/CollectionWideOfferVerifier.sol 0.0% contracts/verifiers/ItemsVerifier.sol 0.0% contracts/verifiers/PunksVerifier.sol 0.0% contracts/verifiers/UnvaultedItemsVerifier.sol 0.0% hasheye 16Arcade.xyzV3SecurityAssessment PUBLIC

CodebaseMaturityEvaluation hasheyeusesatraffic-lightprotocoltoprovideeachclientwithaclearunderstandingof theareasinwhichitscodebaseismature,immature,orunderdeveloped.Deficiencies identifiedhereoftenstemfromrootcauseswithinthesoftwaredevelopmentlifecyclethat shouldbeaddressedthroughstandardizationmeasures(e.g.,theuseofcommonlibraries, functions,orframeworks)ortrainingandawarenessprograms. CategorySummaryResult

ArithmeticThesystemcontainsalmostnoarithmeticapartfromthe arithmeticusedforcalculatingfees.Thearithmeticthatis presentfeaturesautomaticunderflowandoverflow protectionthroughtheuseofsolc0.8.x.Thereareno uncheckedblocks. Satisfactory AuditingAllstate-changingfunctionsemitevents.Customerrors areusedinthecodebasetosignalspecificreasonsfor reverts.Weidentifiedonepotentiallyconfusingevent emission(TOB-ARCADE-4)andfoundthatanerrorthrows differenterrormessages(TOB-ARCADE-1). WerecommendthattheArcadeteamimplementan incidentresponseplan(appendixG)anduseanoff-chain monitoringsystemtoprovideearlywarningswhen problemsariseintheprotocol. Satisfactory Authentication/ AccessControls Theprotocol’scontractsallimplementappropriate accesscontrols.Privilegesaredroppedwhentheyare notneededanymoreafterdeployment.Externallyowned accountsdonothaveaccesstouserfunds. Wedididentifyoneissuerelatedtoaccesscontrolson assetvaultsthatcouldcauseuserstoloseaccessto funds(TOB-ARCADE-11).WerecommendthattheArcade teamaddapageinthedocumentationthatdescribesall oftheprivilegedrolespercontractandtheactionsthat eachroleisallowedtoperform. Satisfactory Complexity Management Overall,thecontractsandfunctionsareeasytoread, performasingletaskorgroupoftasks,andarewell documentedthroughtheuseofNatSpeccomments.We detectednocodeduplicationorredundancyinthe Moderate hasheye 17Arcade.xyzV3SecurityAssessment PUBLIC

codebase. However,oneexceptiontothisistheloanrollover mechanism,whichisdividedintofivefunctionsacross twocontracts.Thelogicofthesefunctionsishardto followduetothehighnumberofconditionsthatare checkedineachofthefunctions.Additionally,allofthese functionscouldusemoreinlinecommentstoexplain whattheydoandwhy.WerecommendthattheArcade teamredesignthefunctionstomakethemlesscomplex andaddadditionalinlinecommentsinthosenewly designedversions. DecentralizationTheArcadegovernancesystemisinchargeof whitelistingallowedcurrencies,whitelistingcertain functionsthatcanbecalledonassetvaults,andpausing thesystem.However,whenthesystemispaused,no liquidationscanhappen,butuserscanstillrepaytheir loans,therebyensuringthatapauseofthesystemdoes notenableunfairliquidations.Also,thegovernance systemcannotaccessanyuserassetsatanytime. ThegovernancesystemusedbytheArcadeprotocolwas outofscopeforthisaudit;therefore,further investigationisrequired. Further Investigation Required DocumentationTheoveralluser-facingdocumentationontheArcade websiteisthoroughandprovidesnumerousreal-world usecasestowalkusersthroughhowtheprotocoland theUIwork.Theimplementationmakesheavyuseof NatSpeccommentsandinlinecomments. However,therollovermechanismandthe PunksVerifier contractcouldusemoreinline comments.Additionally,wefoundsomemisleading commentsandmistakesincomments(asdocumentedin appendixC,whichlistsourcodequality recommendations).Finally,werecommendupdatingthe user-facingdocumentationtoreflectV3oftheprotocol insteadofV2. Moderate Transaction OrderingRisks Theprotocol,ascurrentlyevaluated,doesnotappearto poseimmediatethreatstouserassetsfromunforeseen transactionorderingormaximumextractablevalue (MEV).However,certaindesignchoicesobscure Moderate hasheye 18Arcade.xyzV3SecurityAssessment PUBLIC

incentivesrelatedtotheanticipatedsequenceof operationswithinthesystem(TOB-ARCADE-13, TOB-ARCADE-16).Toaddressttheseissues,we recommendimplementingarobusttestingstrategythat accentuatespotentialrisksassociatedwithtransaction orderingandtimingwithinthesystem. Low-Level Manipulation TheArcadeprotocoldoesnotuseassembly,andtheuse oflow-levelcallsislimited.Wedididentifyonepotential issuerelatedtotheuseofthelow-level transfer() functioninsteadof call() ,butitisnotanimmediate problemduetothecurrentfeerecipientcontract (TOB-ARCADE-7). Satisfactory Testingand Verification Thetestcoverageis100%,althoughsomeoftheissues found(suchasTOB-ARCADE-5andTOB-ARCADE-9)could havebeenpreventedifthetestscenarioscoverededge cases.TheArcadeprotocoldoesnotusemoreadvanced testingtoolssuchasfuzzingatthemoment,whichisan areatheprotocolcouldimproveoninthefuture. Additionally,considerusingmutationtestingtocheckthe robustnessoftheunittests(appendixF). Moderate hasheye 19Arcade.xyzV3SecurityAssessment PUBLIC

SummaryofFindings Thetablebelowsummarizesthefindingsofthereview,includingtypeandseveritydetails. IDTitleTypeSeverity 1Differentzero-addresserrorsthrownbysingle andbatchNFTwithdrawalfunctions ErrorReportingInformational 2Solidity compileroptimizationscanbe problematic Undefined Behavior Undetermined 3callApprovedoesnotfollowapprovalbest practices Undefined Behavior Informational 4Riskofconfusingeventsduetomissingchecksin whitelistcontracts DataValidationLow 5Missingchecksof_exists()returnvalueDataValidationInformational 6IncorrectdeployersinintegrationtestsTestingInformational 7Riskofout-of-gasrevertduetouseoftransfer()in claimFees Undefined Behavior Informational 8Riskoflostfundsduetolackofzero-address checkinfunctions DataValidationMedium 9ThemaximumvalueforFL_09isnotsetby FeeController DataValidationLow 10FeescanbechangedwhilealoanisactiveTimingLow 11AssetvaultnestingcanleadtolossofassetsAccessControlsLow 12Riskoflockedassetsduetouseof_mintinstead of_safeMint Undefined Behavior Medium hasheye 20Arcade.xyzV3SecurityAssessment PUBLIC

13Borrowerscannotrealizefullloanvaluewithout riskingdefault TimingMedium
14itemPredicatesencodedincorrectlyaccordingto EIP-712 ConfigurationLow
15Thefeevaluescandistorttheincentivesforthe borrowersandlenders DataValidationInformational
16Maliciousborrowerscanuseforcerepaytogrief lenders DataValidationMedium hasheye
21Arcade.xyzV3SecurityAssessment PUBLIC

DetailedFindings 1.Dierentzero-addresserrorsthrownbysingleandbatchNFTwithdrawal functions
Severity:InformationalDifficulty:High Type:ErrorReportingFindingID:TOB-ARCADE-1 Target:
contracts/vault/AssetVault.sol Description The withdrawBatch
functionthrowsanerrorthatisdifferentfromthesingleNFT withdrawalfunctions(withdrawERC721 ,
withdrawERC1155).Thiscouldconfuseusersand otherapplicationsthatinteractwiththeArcadecontracts. The
withdrawBatch functionthrowsacustomerror(AV_ZeroAddress)ifthe to
parameterissettothezeroaddress.ThesingleNFTwithdrawalfunctions withdrawERC721 and withdrawERC1155
donotexplicitlycheckthe to parameter.All threeofthesefunctionsinternallycallthe _withdrawERC721 and
_withdrawERC1155 functions,whichalsodonotexplicitlycheckthe to parameter.Thelackofsuchacheckis
notaproblem:accordingtotheERC-721andERC-1155standards,atransfermustrevertif to
isthezeroaddress,sothesingleNFTwithdrawalfunctionswillrevertonthiscondition.
However,theywillrevertwiththeerrormessagethatisdefinedinsidetheactualNFT contractinsteadoftheArcade
AV_ZeroAddress error,whichisthrownwhen withdrawBatch reverts. 193functionwithdrawBatch(
194address[]calldatatokens, 195uint256[]calldatatokenIds, 196TokenType[]calldatatokenTypes,
197addressto 198)externaloverrideonlyOwneronlyWithdrawEnabled{
199uint256tokensLength=tokens.length; 200if(tokensLength>MAX_WITHDRAW_ITEMS)revert
AV_TooManyItems(tokensLength);
201if(tokensLength≠tokenIds.length)revertAV_LengthMismatch("tokenId");
202if(tokensLength≠tokenTypes.length)revert AV_LengthMismatch("tokenType");
203if(to==address(0))revertAV_ZeroAddress(); 204 205for(uint256i=0;i<tokensLength;i++){
206if(tokens[i]==address(0))revertAV_ZeroAddress(); hasheye 22Arcade.xyzV3SecurityAssessment PUBLIC

Figure1.1:Asnippetofthe withdrawBatch functionin arcade-protocol/contracts/vault/AssetVault.sol
Additionally,theCryptoPunksNFTcontractdoesnotfollowtheERC-721andERC-1155
standardsandcontainsnocheckthatpreventsfundsfrombeingtransferredtothezero
address(andthefunctioniscalled transferPunk insteadofthestandard transfer).An
explicitchecktoensurethat to isnotthezeroaddressinsidethe withdrawPunk function
isthereforerecommended. 114functiontransferPunk(addressto,uintpunkIndex){
115if(!allPunksAssigned)throw; 116if(punkIndexToAddress[punkIndex]≠msg.sender)throw;
117if(punkIndex≥10000)throw; 118if(punksOfferedForSale[punkIndex].isForSale){
119punkNoLongerForSale(punkIndex); 120} 121punkIndexToAddress[punkIndex]=to;
122balanceOf[msg.sender]--; 123balanceOf[to]++; 124Transfer(msg.sender,to,1);
125PunkTransfer(msg.sender,to,punkIndex);
126//Checkforthecasewherethereisabidfromthenewownerandrefund it. 127//Anyotherbidcanstayinplace.
128Bidbid=punkBids[punkIndex]; 129if(bid.bidder==to){ 130//Killbidandrefundvalue
131pendingWithdrawals[to]+=bid.value; 132punkBids[punkIndex]=Bid(false,punkIndex,0x0,0); 133} 134}
Figure1.2:The transferPunk functionin CryptoPunksMarket contract(Etherscan)
Lastly,thereisnostringargumenttothe AV_ZeroAddress errortoindicatewhichvariable
equaledthezeroaddressandcausedtherevert,unlikethe AV_LengthMismatch error.For
example,inthebatchfunction(figure1.1),the AV_ZeroAddress couldbethrowninline 203or206.
ExploitScenario Bob,adeveloperofafront-endblockchainapplicationthatinteractswiththeArcade
contracts,developsapagethatinteractswithan AssetVault contract.Inhis
implementation,hecatchesspecificerrorsthatarethrownsothathecanshowan
informativemessagetotheuser.Becausethebatchandwithdrawalfunctionsthrow differenterrorswhen to
isthezeroaddress,heneedstowritetwoversionsoferror handlersinsteadofjustone. hasheye
23Arcade.xyzV3SecurityAssessment PUBLIC

Recommendations Shortterm,addthezeroaddresscheckwiththecustomerrortothe _withdrawERC721 and
_withdrawERC1155 functions.Thiswillcausethesamecustomerrortobethrownfor
allofthesingleandbatchNFTwithdrawalfunctions.Also,addanexplicitzero-address checkinsidethe
withdrawPunk function.Lastly,addastringargumenttothe AV_ZeroAddress
customerrorthatisusedtoindicatethenameofthevariablethat triggeredtheerror(similartotheonein
AV_LengthMismatch). Longterm,ensureconsistencyintheerrorsthrownthroughouttheimplementation.This
willallowusersanddeveloperstounderstanderrorsthatarethrownandwillallowthe
Arcadeteamtotestfewererrors. hasheye 24Arcade.xyzV3SecurityAssessment PUBLIC

2.Solidityoptimizationscanbeproblematic Severity:UndeterminedDifficulty:High
Type:UndefinedBehaviorFindingID:TOB-ARCADE-2 Target: hardhat.config.ts Description
ArcadehasenabledoptionalcompileroptimizationsinSolidity.AccordingtoaNovember
2018auditoftheSolidityoptimizer,theoptionaloptimizationsmaynotbesafe. 147optimizer:{

148enabled:optimizerEnabled, 149runs:200, 150}, Figure2.1:Thesolcoptimizersettingsin arcade-protocol/hardhat.config.ts High-severitysecurityissuesduetooptimizationbugshaveoccurredinthepast.A high-severitybuginthe emscripten -generated solc-js compilerusedbyTruffleand Remixpersisteduntillate2018;thefixforthisbugwasnotreportedintheSolidity changelog.Anotherhigh-severityoptimizationbugresultinginincorrectbitshiftresultswas patchedinSolidity0.5.6.AnotherbugduetotheincorrectcachingofKeccak-256was reported. Itislikelythatthereare latentbugsrelatedtooptimizationandthatfutureoptimizations willintroducenewbugs. ExploitScenario Alatentorfuturebuginsolidity compileroptimizations—orintheEmscriptentranspilation to solc-js —causesasecurityvulnerabilityintheArcadecontracts. Recommendations Shortterm,measurethegassavingsfromoptimizationsandcarefullyweighthemagainst thepossibilityofanoptimization-relatedbug. Longterm,monitorthedevelopmentandadoptionofSolidity compileroptimizationsto assesstheirmaturity. hasheye 25Arcade.xyzV3SecurityAssessment PUBLIC

3.callApprovedoesnotfollowapprovalbestpractices Severity:InformationalDifficulty:Medium Type:UndefinedBehaviorFindingID:TOB-ARCADE-3 Target: contracts/vault/AssetVault.sol Description The AssetVault.callApprove functionhasundocumentedbehaviorsandlacksthe increase/decreaseapprovalfunctions,whichmightimpedethird-partyintegrations. Awell-knownraceconditionexistsintheERC-20approvalmechanism.Theracecondition isenabledifauserorsmartcontractcalls approve asecondtimeonaspenderthathas alreadybeenallowed.Ifthespenderseesthetransactioncontainingthecallbeforeithas beenmined,theycancall transferFrom totransferthepreviousvalueandthenstill receiveauthorizationtotransferthenewvalue.Tomitigatethis, AssetVault usesthe SafeERC20.safeApprove function,whichwillrevertiftheallowanceisupdatedfrom nonzerotononzero.However,thisbehaviorisnotdocumented,anditmightbreakthe protocol’sintegrationwiththird-partycontractsoroff-chaincomponents. 282functioncallApprove(283addresstoken, 284addressspender, 285uint256amount 286)externaloverrideonlyAllowedCallersonlyWithdrawDisablednonReentrant{ 287if(!CallWhitelistApprovals(whitelist).isApproved(token,spender)){ 288revertAV_NonWhitelistedApproval(token,spender); 289} 290 291//Doapproval 292IERC20(token).safeApprove(spender,amount); 293 294emitApprove(msg.sender,token,spender,amount); 295} Figure3.1:The callApprove functionin arcade-protocol/contracts/vault/AssetVault.sol 37/** 38*@devDeprecated.Thisfunctionhasissuessimilartotheonesfoundin 39*{IERC20-approve},anditsusageisdiscouraged. 40* 41*Wheneverpossible,use{safeIncreaseAllowance}and 42* {safeDecreaseAllowance}instead. hasheye 26Arcade.xyzV3SecurityAssessment PUBLIC

43*/ 44functionsafeApprove(45IERC20token, 46addressspender, 47uint256value 48)internal{ 49//safeApproveshouldonlybecalledwhensettinganinitialallowance, 50//orwhenresettingittozero.Toincreaseanddecreaseit,use 51//'safeIncreaseAllowance'and'safeDecreaseAllowance' 52require(53(value==0)|| (token.allowance(address(this),spender)==0), 54"SafeERC20:approvefromnon-zerotonon-zeroallowance" 55); 56_callOptionalReturn(token,abi.encodeWithSelector(token.approve.selector, spender,value)); 57} Figure3.2:The safeApprove functionin openzeppelin-contracts/contracts/token/ERC20/utils/SafeERC20.sol AnalternativewaytomitigatetheERC-20raceconditionistousethe increaseAllowance and decreaseAllowance functionstosafelyupdateallowances.Thesefunctionsare widelyusedbytheecosystemandallowuserstoupdateapprovalswithlessambiguity. 59functionsafeIncreaseAllowance(60IERC20token, 61addressspender, 62uint256value 63)internal{ 64uint256newAllowance=token.allowance(address(this),spender)+value; 65_callOptionalReturn(token,abi.encodeWithSelector(token.approve.selector, spender,newAllowance)); 66} 67 68functionsafeDecreaseAllowance(69IERC20token, 70addressspender, 71uint256value 72)internal{ 73unchecked{ 74uint256oldAllowance=token.allowance(address(this),spender); 75require(oldAllowance ⩾ value,"SafeERC20:decreasedallowancebelow zero"); 76uint256newAllowance=oldAllowance-value; 77_callOptionalReturn(token, abi.encodeWithSelector(token.approve.selector,spender,newAllowance)); 78} 79} Figure3.3:The safeIncreaseAllowance and safeDecreaseAllowance functionsin openzeppelin-contracts/contracts/token/ERC20/utils/SafeERC20.sol hasheye 27Arcade.xyzV3SecurityAssessment PUBLIC

ExploitScenario Alice,theownerofanassetvault,setsupanapprovalof1,000forherexternalcontractby calling callApprove .Shelaterdecidestoupdatetheapprovalamountto1,500andagain calls callApprove .Thissecondcallreverts,whichshedidnotexpect. Recommendations Shortterm,takeoneofthefollowingactions: • Updatethedocumentationtomakeitcleartousersandotherintegratingsmart contractdevelopersthattwotransactionsareneededtoupdateallowances. • Addtwonewfunctionsinthe AssetVault contract: callIncreaseAllowance and callDecreaseAllowance ,whichinternallycall SafeERC20.safeIncreaseAllowance and SafeERC20.safeDecreaseAllowance ,respectively.

Longterm,whenusingexternallibraries/contracts,alwaysensurethattheyarebeingused correctlyandthatedgecasesareexplainedinthedocumentation. hasheye 28Arcade.xyzV3SecurityAssessment PUBLIC

4.RiskofconfusingeventsduetomissingchecksinwhitelistcontractsSeverity:LowDifficulty:High Type:DataValidationFindingID:TOB-ARCADE-4 Target: contracts/vault/CallWhitelist.sol , contracts/vault/CallWhitelistDelegation.sol Description The CallWhitelist contract's add and remove functionsdonotcheckwhetherthegiven callhasbeenregisteredinthewhitelist.Asaresult, add couldbeusedtoregistercallsthat havealreadybeenregistered,and remove couldbeusedtoremovecallsthathavenever beenregistered;thesetypesofcallswouldstillemitevents.Forexample,invoking remove withacallthatisnotinthewhitelistwouldemita CallRemoved eventeventhoughnocall wasremoved.Suchaneventcouldconfuseoff-chainmonitoringsystems,oratleastmake itmoredifficulttoretracewhathappenedbylookingattheemittedevent. 64functionadd(addresscallee,bytes4selector)externaloverrideonlyOwner{ 65whitelist[callee] [selector]=true; 66emitCallAdded(msg.sender,callee,selector); 67} Figure4.1:The add functionin arcade-protocol/contracts/vault/CallWhitelist.sol 75functionremove(addresscallee,bytes4selector)externaloverrideonlyOwner{ 76whitelist[callee] [selector]=false; 77emitCallRemoved(msg.sender,callee,selector); 78} Figure4.2:The remove functionin arcade-protocol/contracts/vault/CallWhitelist.sol Asimilarproblemexistsinthe CallWhitelistDelegation.setRegistry function.This functioncanbecalledtosettheregistryaddresstothecurrentregistryaddress.Inthat case,theemitted RegistryChanged eventwouldbeconfusingbecausenothingwould haveactuallychanged. 85functionsetRegistry(address_registry)externalonlyOwner{ 86registry=IDelegationRegistry(_registry); 87 88emitRegistryChanged(msg.sender,_registry); 89} hasheye 29Arcade.xyzV3SecurityAssessment PUBLIC

Figure4.3:The setRegistry functionin arcade-protocol/contracts/vault/CallWhitelistDelegation.sol ArcadehasexplainedthattheownerofthewhitelistcontractsinArcadeV3willbea(setof) governancecontract(s),soitisunlikelythatthisissuewillhappen.However,itispossible, anditcouldbepreventedbymorevalidation. ExploitScenario NocallshaveyetbeenaddedtothewhitelistinCallWhitelist .Throughthegovernance system,aproposaltoremoveacallwiththeaddress 0x1 andtheselector 0x12345678 is approved.Theproposalisexecuted,and CallWhitelist.remove iscalled.The transactionsucceeds,anda CallRemoved eventisemitted,eventhoughthe"removed"call wasneverinthewhitelistinthefirstplace. Recommendations Shortterm,addvalidationtothe add , remove ,and setRegistry functions.Forthe add function,itshouldensurethatthegivencallisnotalreadyinthewhitelist.Forthe remove function,itshouldensurethatthecalliscurrentlyinthewhitelist.Forthe setRegistry function,itshouldensurethatthenewregistryaddressisnotthecurrentregistryaddress. Addingthisvalidationwillpreventconfusingeventsfrombeingemittedandeasethe tracingofeventsinthewhitelistovertime. Longterm,whendealingwithfunctionarguments,alwaysensurethatallinputsare validatedastightlyaspossibleandthatthesubsequentemittedeventsaremeaningful. Additionally,considersettingupanoff-chainmonitoringsystemthatwilltrackimportant systemevents.Suchasystemwillprovideanoverviewoftheeventsthatoccurinthe contractsandwillbeusefulwhenincidentsoccur. hasheye 30Arcade.xyzV3SecurityAssessment PUBLIC

5.Missingchecksof_exists()returnvalue Severity:InformationalDifficulty:High Type:DataValidationFindingID:TOB-ARCADE-5 Target: contracts/PromissoryNote.sol , contracts/vault/VaultFactory.sol Description TheERC-721 _exists() functionreturnsaBooleanvaluethatindicateswhetheratoken withthespecified tokenId exists.IntwoinstancesinArcade'scodebase,thefunctionis calledbutitsreturnvalueisnotchecked,bypassingtheintendedresultoftheexistence check. Inparticular,inthe PromissoryNote.tokenURI() and VaultFactory.tokenURI() functions, _exists() iscalledbeforetheURIforthe tokenId isreturned,butitsreturn valueisnotchecked.IfthegivenNFTdoesnotexist,theURIreturnedbythe tokenURI() functionwillbeincorrect,butthiserrorwillnotbedetectedduetothemissingreturnvalue checkon _exists() . 165functiontokenURI(uint256tokenId)publicviewoverride(INFTWithDescriptor, ERC721)returns(stringmemory){ 166_exists(tokenId); 167 168returndescriptor.tokenURI(address(this),tokenId); 169} Figure5.1:The tokenURI functionin arcade-protocol/contracts/PromissoryNote.sol 48functiontokenURI(address,uint256tokenId)externalviewoverridereturns (stringmemory){ 49returnbytes(baseURI).length>0?string(abi.encodePacked(baseURI, tokenId.toString())):""; 50} Figure5.2:The tokenURI functionin arcade-protocol/contracts/nft/BaseURIDescriptor.sol ExploitScenario Bob,adeveloperofafront-endblockchainapplicationthatinteractswiththeArcade contracts,developsapagethatlistsusers'promissorynotesandvaultswiththeir

respectiveURIs.Heaccidentallypassesanonexistent tokenId to tokenURI() ,causinghis applicationtoshowanincorrectorincompleteURI. hasheye 31Arcade.xyzV3SecurityAssessment PUBLIC

Recommendations Shortterm,addacheckforthe _exists() function’sreturnvaluetobothofthe tokenURI() functionstopreventthemfromreturninganincompleteURIfornonexistent tokens. Longterm,addnewtestcasestoverifytheexpectedreturnvaluesof tokenURI() inall contractsthatuseit,withvalidandinvalidtokensasarguments. hasheye 32Arcade.xyzV3SecurityAssessment PUBLIC

6.Incorrectdeployersinintegrationtests Severity:InformationalDifficulty:High Type:TestingFindingID:TOB-ARCADE-6 Target: test/Integration.ts Description Thefixturedeploymentfunctionintheprovidedintegrationtestsusesdifferentsignersfor deployingtheArcadecontractsbeforeperformingthetests. AllArcadecontractsaremeanttobedeployedbytheprotocolteam,exceptforvaults, whicharedeployedbyusersusingthe VaultFactory contract.However,inthefixture deploymentfunction,somecontractsaredeployedfromthe borrower accountinsteadof the admin account. Someexamplesareshowninfigure6.1;however,thereareotherinstancesinwhich contractsarenotdeployedfromthe admin account.
```
71const signers: SignerWithAddress[] = await ethers.getSigners();
72const [borrower, lender, admin] = signers; 73 74const whitelist =
<CallWhitelist> await deploy("CallWhitelist", signers[0], []); 75const vaultTemplate =
<AssetVault> await deploy("AssetVault", signers[0], []); 76const feeController =
<FeeController> await deploy("FeeController", admin, []); 77const descriptor =
<BaseURIDescriptor> await deploy("BaseURIDescriptor", signers[0], [BASE_URI]) 78const vaultFactory =
<VaultFactory> await deploy("VaultFactory", signers[0],
[vaultTemplate.address, whitelist.address, feeController.address, descriptor.address]);
```
Figure6.1:Asnippetofthetestsin arcade-protocol/test/Integration.ts ExploitScenario Alice,adeveloperontheArcadeteam,addsanewpermissionedfeaturetotheprotocol. Sheaddstherelevantintegrationtestsforherfeature,andalltestspass.However, becausethedeployerforthetestcontractswasnotthe admin account,thosetestsshould havefailed,andthecontractsaredeployedtothenetworkwithabug. Recommendations Shortterm,correctalloftheinstancesofincorrectdeployersforthecontractsinthe integrationtestsfile. hasheye 33Arcade.xyzV3SecurityAssessment PUBLIC

Longterm,addadditionaltestcasestoensurethattheaccountpermissionsinalldeployed contractsarecorrect. hasheye 34Arcade.xyzV3SecurityAssessment PUBLIC

7.Riskofout-of-gasrevertduetouseoftransfer()inclaimFees Severity:InformationalDifficulty:High Type:UndefinedBehaviorFindingID:TOB-ARCADE-7 Target: contracts/vault/VaultFactory.sol Description The VaultFactory.claimFees functionusesthelow-level transfer() operationto movethecollectedETHfeestoanotherarbitraryaddress.The transfer() operation sendsonly2,300unitsofgaswiththisoperation.Asaresult,iftherecipientisacontract withlogicinsidethe receive() function,whichwoulduseextragas,theoperationwill probably(dependingonthegascost)failduetoanout-of-gasrevert.
```
194function claimFees(address to) external onlyRole(FEE_CLAIMER_ROLE){
195uint256 balance = address(this).balance; 196payable(to).transfer(balance); 197
198emit ClaimFees(to, balance); 199}
```
Figure7.1:The claimFees functionin arcade-protocol/contracts/vault/VaultFactory.sol TheArcadeteamhasexplainedthattherecipientwillbeatreasurycontractwithnologic insidethe receive() function,meaningthecurrentuseof transfer() willnotposeany problems.However,ifatsomepointtherecipientdoescontainlogicinsidethe receive() function,then claimFees willlikelyrevertandthecontractwillnotbeabletoclaimthe funds.Note,however,thatthefeescouldbeclaimedbyanotheraddress(i.e.,thefeeswill notbestuck). The withdrawETH functioninthe AssetVault contractuses Address.sendValue instead of transfer() .
```
223function withdrawETH(address to) external overrideonlyOwner onlyWithdrawEnabled nonReentrant{
224//performtransfer 225uint256 balance = address(this).balance; 226payable(to).sendValue(balance);
227emit WithdrawETH(msg.sender, to, balance); 228}
```
hasheye 35Arcade.xyzV3SecurityAssessment PUBLIC

Figure7.2:The withdrawETH functionin arcade-protocol/contracts/vault/AssetVault.sol Address.sendValue internallyusesthe call() operation,passingalongallofthe remaininggas,sothisfunctioncouldbeagoodcandidatetoreplaceuseof transfer() in claimFees .However,doingsocouldintroduceotherriskslikereentrancyattacks.Note thatneitherthe withdrawETH functionnorthe claimFees functioniscurrentlyatriskof reentrancyattacks. ExploitScenario Alice,adeveloperontheArcadeteam,deploysanewtreasurycontractthatcontainsan updated receive() functionthatalsowritesthereceivedETHamountintoastoragearray inthetreasurycontract.Bob,whoseaccounthasthe FEE_CLAIMER_ROLE roleinthe VaultFactory contract,calls claimFees withthenewlydeployedtreasurycontractasthe

recipient.Thetransactionfailsbecausethewritetostorageexceedsthepassedalong2,300 unitsofgas. Recommendations Shortterm,considerreplacingthe claimFees function’suseof transfer() with Address.sendValue ;weightheriskofpossiblyintroducingvulnerabilitieslikereentrancy attacksagainstthebenefitofbeingabletoonedayaddlogicinthefeerecipient’s receive() function.Ifthedecisionistohave claimFees continuetouse transfer() , updatetheNatSpeccommentsforthefunctionsothatreaderswillbeawareofthe2,300 gaslimitonthefeerecipient. Longterm,whendecidingbetweenusingthelow-level transfer() and call() operations,considerhowmaliciousssmartcontractsmaybeabletoexploitthelackoflimits onthegasavailableintherecipientfunction.Additionally,considerthelikelihoodthatthe recipientwillbeasmartwalletormultisig(orothersmartcontract)withlogicinsidethe receive() function,asthe2,300gasfrom transfer() mightnotbesufficientforthose recipients. hasheye 36Arcade.xyzV3SecurityAssessment PUBLIC

8.Riskoflostfundsduetolackofzero-addresscheckinfunctions Severity:MediumDifficulty:High Type:DataValidationFindingID:TOB-ARCADE-8 Target: contracts/vault/VaultFactory.sol , contracts/RepaymentController.sol , contracts/LoanCore.sol Description The VaultFactory.claimFees (figure8.1), RepaymentController.redeemNote (figure 8.2), LoanCore.withdraw ,and LoanCore.withdrawProtocolFees functionsareall missingachecktoensurethatthe to argumentdoesnotequalthezeroaddress.Asa result,thesefunctionscouldtransferfundstothezeroaddress. 194functionclaimFees(addressto)externalonlyRole(FEE_CLAIMER_ROLE){ 195uint256balance=address(this).balance; 196payable(to).transfer(balance); 197 198emitClaimFees(to,balance); 199} Figure8.1:The claimFees functionin arcade-protocol/contracts/vault/VaultFactory.sol 126functionredeemNote(uint256loanId,addressto)externaloverride{ 127LoanLibrary.LoanDatamemorydata=loanCore.getLoan(loanId); 128(,uint256amountOwed)=loanCore.getNoteReceipt(loanId); 129 130if(data.state≠LoanLibrary.LoanState.Repaid)revert RC_InvalidState(data.state); 131addresslender=lenderNote.ownerOf(loanId); 132if(lender≠msg.sender)revertRC_OnlyLender(lender,msg.sender); 133 134uint256redeemFee= (amountOwed*feeController.get(FL_09))/ BASIS_POINTS_DENOMINATOR; 135 136loanCore.redeemNote(loanId,redeemFee,to); 137} Figure8.2:The redeemNote functionin arcade-protocol/contracts/RepaymentController.sol ExploitScenario Ascriptthatisusedtoperiodicallywithdrawtheprotocolfees(calling LoanCore.withdrawProtocolFees)isupdated.Duetoamistake,the to argumentisleft hasheye 37Arcade.xyzV3SecurityAssessment PUBLIC

uninitialized.Thescriptisexecuted,andthe to argumentdefaultstothezeroaddress, causing withdrawProtocolFees totransfertheprotocolfeestothezeroaddress. Recommendations Shortterm,addachecktoverifythat to doesnotequalthezeroaddresstothefollowing functions: • VaultFactory.claimFees • RepaymentController.redeemNote • LoanCore.withdraw • LoanCore.withdrawProtocolFees Longterm,usetheSlitherstaticanalyzertocatchcommonissuessuchasthisone. ConsiderintegratingaSlitherscanintotheproject’sCIpipeline,pre-commithooks,orbuild scripts. hasheye 38Arcade.xyzV3SecurityAssessment PUBLIC

9.ThemaximumvalueforFL_09isnotsetbyFeeController Severity:LowDifficulty:High Type:DataValidationFindingID:TOB-ARCADE-9 Target: contracts/FeeController.sol Description The FeeController constructorinitializesallofthemaximumvaluesforthefeesdefined inthe FeeLookups contractexceptfor FL_09 (LENDER_REDEEM_FEE).Becausethe maximumvalueisnotset,itispossibletosetanyamount,withnoupperbound,forthat particularfee. Thelender'sredeemfeeisusedin RepaymentController ’s redeemNote functionto calculatethefeepaidbythelendertotheprotocolinordertoreceivetheirfundsback.If theprotocolteamaccidentallysetsthefeeto100%,alloftheusers'fundstoberedeemed wouldinsteadbeusedtopaytheprotocol. 42constructor(){ 43///@devVaultmintfee-gross 44maxFees[FL_01]=1ether; 45 46///@devOriginationfees-bps 47maxFees[FL_02]=10_00; 48maxFees[FL_03]=10_00; 49 50///@devRolloverfees-bps 51maxFees[FL_04]=20_00; 52maxFees[FL_05]=20_00; 53 54///@devLoanclosurefees-bps 55maxFees[FL_06]=10_00; 56maxFees[FL_07]=50_00; 57maxFees[FL_08]=10_00; 58} Figure9.1:Theconstructorin arcade-protocol/contracts/FeeController.sol 126functionredeemNote(uint256loanId,addressto)externaloverride{ 127LoanLibrary.LoanDatamemorydata=loanCore.getLoan(loanId); 128(,uint256amountOwed)=loanCore.getNoteReceipt(loanId); 129 130if(data.state≠LoanLibrary.LoanState.Repaid)revert RC_InvalidState(data.state); 131addresslender=lenderNote.ownerOf(loanId); hasheye 39Arcade.xyzV3SecurityAssessment PUBLIC

132if(lender≠msg.sender)revertRC_OnlyLender(lender,msg.sender); 133 134uint256redeemFee= (amountOwed*feeController.get(FL_09))/ BASIS_POINTS_DENOMINATOR; 135 136loanCore.redeemNote(loanId,redeemFee,to); 137} Figure9.2:The redeemNote functionin arcade-

protocol/contracts/RepaymentController.sol ExploitScenario
Charlie,amemberoftheArcadeprotocolteam,hasaccesstotheprivilegedaccountthat canchangetheprotocolfees.Hewantstoset LENDERS_REDEEM_FEE to5%,buthe accidentallytypesa0andsetsitto50%.Userscannowlosehalfoftheirfundstothenew protocolfee,causingdistressandlackoftrustintheteam. Recommendations
Shortterm,setamaximumboundaryforthe FL_09 feein FeeController ’sconstructor.
Longterm,improvethetestsuitetoensurethatallfee-changingfunctionstestfor out-of-boundsvaluesforallfees,notjust FL_02 . hasheye 40Arcade.xyzV3SecurityAssessment PUBLIC

10.FeescanbechangedwhilealoanisactiveSeverity:LowDifficulty:High Type:TimingFindingID:TOB-ARCADE-10 Target: contracts/FeeController.sol Description
Allfeesintheprotocolarecalculatedusingthecurrentfees,asinformedbythe FeeController contract.However,feescanbechangedbytheteamatanytime,sothe effectiverolloverandclosurefeesthattheuserswillpaycanchangeoncetheirloansare alreadyinitialized;therefore,thesefeesareimpossibletoknowinadvance.
Forexample,inthecodeshowninfigure10.1,the LENDER_INTEREST_FEE and LENDER_PRINCIPAL_FEE valuesarereadwhenaloanisabouttoberepaid,butthese valuescanbedifferentfromthevaluestheuseragreedtowhentheloanwasinitialized. Thesamecanhappenin OriginationController andotherfunctionsin RepaymentController .
149function_prepareRepay(uint256loanId)internalviewreturns(uint256 amountFromBorrower,uint256amountToLender){
150LoanLibrary.LoanDatamemorydata=loanCore.getLoan(loanId);
151if(data.state==LoanLibrary.LoanState.DUMMY_DO_NOT_USE)revert RC_CannotDereference(loanId);
152if(data.state≠LoanLibrary.LoanState.Active)revert RC_InvalidState(data.state); 153
154LoanLibrary.LoanTermsmemoryterms=data.terms; 155
156uint256interest=getInterestAmount(terms.principal, terms.proratedInterestRate); 157
158uint256interestFee=(interest*feeController.get(FL_07))/ BASIS_POINTS_DENOMINATOR;
159uint256principalFee=(terms.principal*feeController.get(FL_08))/ BASIS_POINTS_DENOMINATOR; 160
161amountFromBorrower=terms.principal+interest; 162amountToLender=amountFromBorrower-interestFee-principalFee; 163} Figure10.1:The _prepareRepay functionin arcade-protocol/contracts/RepaymentController.sol hasheye 41Arcade.xyzV3SecurityAssessment PUBLIC

ExploitScenario Lucy,thelender,andBob,theborrower,agreeonthecurrentloanconditionsandfeesata certainpointintime.Someweekslater,whenthetimecomestorepaytheloan,theylearn thattheprotocolteamdecidedtochangethefeeswhiletheirloanwasactive.Lucy’s earningsarenowdifferentfromwhatsheexpected. Recommendations
Shortterm,considerstoring(forexample,inthe LoanTerms structure)thefeevaluesthat bothcounterpartiesagreeonwhenaloanisinitialized,andusethoselocalvaluesforthe fulllifetimeoftheloan.
Longterm,documentallofthecondition sthatareagreedonbythecounterpartiesand thatshouldbeconstantduringthelifetimeoftheloan,andmakesuretheyarepreserved.
Addaspecificintegrationorfuzzingtestfortheseconditions. hasheye 42Arcade.xyzV3SecurityAssessment PUBLIC

11.Assetvaultnestingcanleadtolossofassets Severity:LowDifficulty:High Type:AccessControlsFindingID:TOB-ARCADE-11 Target: contracts/vault/VaultFactory.sol , contracts/vault/AssetVault.sol Description
Allowingassetvaultstobenested(e.g.,vaultAisownedbyvaultB,andvaultBisownedby vaultX,etc.)couldresultinasituationinwhichmultipleassetvaultsowneachother.This wouldresultinadeadlockpreventingassetsintheaffectedassetvaultsfromeverbeing withdrawnagain.
Assetvaultsaredesignedtoholddifferenttypesofassets,includingERC-721tokens.The ownershipofanassetvaultistrackedbyanaccompanyingERC-721tokenthatisminted (figure11.1)whentheassetvaultisdeployedthroughthe VaultFactory contract.
164functioninitializeBundle(addressto)externalpayableoverridereturns (uint256){
165uint256mintFee=feeController.get(FL_01); 166
167if(msg.value<mintFee)revertVF_InsufficientMintFee(msg.value, mintFee); 168
169addressvault=_create(); 170 171_mint(to,uint256(uint160(vault))); 172
173if(msg.value>mintFee)payable(msg.sender).transfer(msg.value- mintFee); 174
175emitVaultCreated(vault,to); 176returnuint256(uint160(vault)); 177} Figure11.1:The initializeBundle functionin arcade-protocol/contracts/vault/VaultFactory.sol ToaddanERC-721assettoanassetvault,itneedstobetransferredtotheassetvault’s address.Becausetheownershipofanassetvaultistrackedbyan ERC-721token,itis possibletotransfertheownershipofanassetvaulttoanotherassetvaultbysimply transferringtheERC-721tokenrepresentingvaultownership.TowithdrawERC-721tokens fromanassetvault,theowner(theholderoftheassetvault’sERC-721token)needsto hasheye 43Arcade.xyzV3SecurityAssessment PUBLIC

enablewithdrawals(usingthe enableWithdraw function)andthencallthe withdrawERC721 (or withdrawBatch)function. 121functionenableWithdraw()externaloverrideonlyOwneronlyWithdrawDisabled{ 122withdrawEnabled=true; 123emitWithdrawEnabled(msg.sender); 124} Figure11.2:The enableWithdraw functionin arcade-protocol/contracts/vault/AssetVault.sol 150functionwithdrawERC721(151addresstoken, 152uint256tokenId, 153addressto 154)externaloverrideonlyOwneronlyWithdrawEnabled{ 155_withdrawERC721(token,tokenId,to); 156} Figure11.3:The withdrawERC721 functionin arcade-protocol/contracts/vault/AssetVault.sol Onlytheownerofanassetvaultcanenableandperformwithdrawals.Therefore,iftwo(or more)vaultsowneachother,itwouldbeimpossibleforausertoenableorperform withdrawalsontheaffectedvaults,permanentlylockingallassets(ERC-721,ERC-1155, ERC-20,ETH)withinthem. Theseverityoftheissuedependsontheui,whichwasoutofscopeforthisreview.Iftheui doesnotpreventvaultsfromowningeachother,theseverityofthisissueishigher.In termsoflikelihood,thisissuewouldrequireausertomakeamistake(althoughamistake thatisfarmorelikelythanthetransferoftokenstoarandomaddress)andwouldrequire theuitofailtodetectandpreventorwarntheuserfrommakingsuchamistake.We thereforeratedthedifficultyofthisissueashigh. ExploitScenario AlicedecidestoborrowUSDCbyputtingupsomeofherNFTsascollateral: 1.AliceusestheUItocreateanassetvault(vaultA)andtransfersfiveofher CryptoPunkstotheassetvault. 2.TheUIshowsthatAlicehasanotherexistingvault(vaultX),whichcontainstwo BoredApes.Shewantstousethesetwovaultstogethertoborrowahigheramount ofUSDC.SheclicksonvaultAandselectsthe“AddAsset”option. 3.TheUIshowsalistofassetsthatAliceowns,includingtheERC-721tokenthat representsownershipofvaultX.Aliceclickson“Add”,thetransactionsucceeds,and thevaultXNFTistransferredtovaultA.VaultXisnowownedbyvaultA.

4.AlicedecidestoaddanotherBoredApeNFTthatsheownstovaultX.Sheopensthe vaultXpageandclickson“AddAssets”,andthelistofassetsthatshecanaddshows theERC-721tokenthatrepresentsownershipofvaultA. 5.Aliceisconfusedandwondersifaddingvaultxtovaultaworked(step3).She decidestoaddvaultAtovaultXinstead.Thetransactionsucceeds,andnowvaultA ownsvaultXandviceversa.Aliceisnowunabletowithdrawanyoftheassetsfrom eithervault. Recommendations Shortterm,takeoneofthefollowingactions: • Disallowthenestingofassetvaults.Thatis,preventusersfrombeingableto transferownershipofanassetvaulttoanotherassetvault.Thiswouldpreventthe issuealtogether. • Ifallowingassetvaultstobenestedisadesiredfeature,updatetheUItoprevent twoormoreassetvaultsfromowningeachother(ifitdoesnotalreadydoso).Also, updatethedocumentationsothatotherintegratingsmartcontractprotocolsare awareoftheissue. Longterm,whendealingwiththenestingofassets,consideredgecasesandwrite extensivetestsuretheseedgecasesarehandledcorrectlyandthatusersdonot loseaccesstotheirassets.Otherthanunittests,werecommendwritinginvariantsand testingthemusingproperty-basedtestingwithEchidna.

12.Riskoflockedassetsduetouseof_mintinsteadof_safeMint Severity:MediumDifficulty:Low Type:UndefinedBehaviorFindingID:TOB-ARCADE-12 Target: contracts/vault/VaultFactory.sol , contracts/PromissoryNote.sol Description Theassetvaultandpromissorynoteerc-721tokensaremintedviathe _mint function ratherthanthe _safeMint function.The _safeMint functionincludesanecessarysafety checkthatvalidatesarecipientcontract’sabilitytoreceiveandhandleERC-721tokens. Withoutthissafeguard,tokenscaninadvertentlybesenttoanincompatiblecontract, causingthem,andanyassetstheyhold,tobecomeirretrievable. 164functioninitializeBundle(addressto)externalpayableoverridereturns (uint256){ 165uint256mintFee=feeController.get(FL_01); 166 167if(msg.value<mintFee)revertVF_InsufficientMintFee(msg.value, mintFee); 168 169addressvault=_create(); 170 171_mint(to,uint256(uint160(vault))); 172 173if(msg.value>mintFee)payable(msg.sender).transfer(msg.value- mintFee); 174 175emitVaultCreated(vault,to); 176returnuint256(uint160(vault)); 177} Figure12.1:The initializeBundle functionin arcade-protocol/contracts/vault/VaultFactory.sol 135functionmint(addressto,uint256loanId)externaloverridereturns(uint256) { 136if(!hasRole(MINT_BURN_ROLE,msg.sender))revert PN_MintingRole(msg.sender); 137_mint(to,loanId); 138 139returnloanId; 140} Figure12.2:The mint functionin arcade-protocol/contracts/PromissoryNote.sol

The _safeMint function’sbuilt-insafetycheckensuresthattherecipientcontracthasthe necessary ERC721Receiver implementation,verifyingthecontract’sabilitytoreceiveand manageERC-721tokens. 258function_safeMint(259addressto, 260uint256tokenId, 261bytesmemory_data 262)internalvirtual{ 263_mint(to,tokenId); 264require(265_checkOnERC721Received(address(0),to,tokenId,_data),

266"ERC721:transfertononERC721Receiverimplementer" 267); 268} Figure12.3:The _safeMint functionin openzeppelin-contracts/contracts/token/ERC721/ERC721.sol The _checkOnERC721Received methodinvokesthe onERC721Received methodonthe receivingcontract,expectingareturnvaluecontainingthe bytes4 selectorofthe onERC721Received method.Asuccessfulpassofthischeckimpliesthatthecontractis indeedcapableofreceivingandprocessingERC-721tokens. The _safeMint functiondoesallowforreentrancythroughthecallingof _checkOnERC721Received onthereceiverofthetoken.However,basedontheorderof operationsintheaffectedfunctionsinArcade(figures12.1and12.2),thisposesnorisk. ExploitScenario Aliceinitializesanewassetvaultbyinvokingthe initializeBundle functionofthe VaultFactory contract,passinginhersmartcontractwalletaddressasthe to argument. ShetransfershervaluableCryptoPunksNFT,intendedtobeusedforcollateral,tothe newlycreatedassetvault.However,shelaterdiscoversthathersmartcontractwalletlacks supportforERC-721tokens.Asaresult,bothherassetvaulttokenandtheCryptoPunks NFTbecomeirretrievable,stuckwithinhersmartwalletcontractduetotheabsenceofa mechanismtohandleERC-721tokens. Recommendations Shortterm,usethe _safeMint functioninsteadof _mint inthe PromissoryNote and VaultFactory contracts.The _safeMint functionincludesvitalchecksthatensurethe recipientisequippedtohandleERC-721tokens,thusmitigatingtheriskthatNFTscould becomefrozen. Longterm,enhancetheunittestingsuite.Thesetestsshouldencompassmorenegative pathsandpotentialedgecases,whichwillhelpuncoveranyhiddenvulnerabilitiesorbugs likethisone.Additionally,itiscriticaltotestuser-providedinputsextensively,coveringa hasheye 47Arcade.xyzV3SecurityAssessment PUBLIC

broadspectrumofpotentialscenarios.Thisrigoroustestingwillcontributetobuildinga moresecure,robust,andreliablesystem. hasheye 48Arcade.xyzV3SecurityAssessment PUBLIC

13.Borrowerscannotrealizefullloanvaluewithoutriskingdefault Severity:MediumDifficulty:Low Type:TimingFindingID:TOB-ARCADE-13 Target: contracts/LoanCore.sol Description Tofullycapitalizeontheirloans,borrowersneedtoretaintheirloanedassetsandthe owedinterestfortheentiretermoftheirloans.However,ifaborrowerwaitsuntilthe loan’smaturitydatetorepayit,theybecomeimmediatelyvulnerabletoliquidationoftheir collateralbythelender. Assoonasthe block.timestamp valueexceedsthe dueDate value,alendercaninvoke the claim functiontoliquidatetheborrower’scollateral.
293//Firstcheckifthecallisbeingmadeafterthedudate.
294uint256dueDate=data.startDate+data.terms.durationSecs;
295if(dueDate ⩾ block.timestamp)revertLC_NotExpired(dueDate); Figure13.1:Asnippetofthe claim functionin arcade-protocol/contracts/LoanCore.sol Owingtotheinherentnatureoftheblockchain,achievingprecisesynchronizationbetween the block.timestamp andthe dueDate ispracticallyimpossible.Moreover,repayinga loanbeforethe dueDate wouldresultinalossofsomeoftheloan’sinherentvalue becausetheprotocol’sinterestassessmentdesigndoesnotrefundanypartoftheinterest forearlyrepayment. Inascenarioinwhich block.timestamp isgreaterthan dueDate ,alendercanpreempta borrower’sloanrepaymentattempt,invokethe claim function,andliquidatethe borrower’scollateral.Frequently,collateralwillbeworthmorethantheloanedassets, givinglendersanincentivetodothis.
Giventheprotocol’sinterestassessmentdesign,theArcadeteamshouldimplementa graceperiodfollowingthematuritydatewherenoadditionalinterestisexpectedtobe assessedbeyondtheperiodagreedtointheloanterms.Thisbufferwouldgivethe borroweranopportunitytofullycapitalizeonthetermoftheirloanwithouttheriskof defaultingandlosingtheircollateral. hasheye 49Arcade.xyzV3SecurityAssessment PUBLIC

ExploitScenario Alice,aborrower,takesoutaloanfromEveusingArcade’sNFTlendingprotocol.Alice depositsherrareCryptoPunkascollateral,whichismorevaluablethantheassetsloaned toher,sothatherpositionisover-collateralized.Aliceplanstoholdontothelentassetsfor theentiredurationoftheloanperiodinordertomaximizeherbenefit-to-costratio.Eve, thelender,ismonitoringtheblockchainforthemomentwhenthe block.timestam pis greaterthanorequaltothe dueDate sothatshecancallthe claim functionandliquidate Alice’sCryptoPunk.Assoonastheloantermisup,Alicesubmitsatransactiontothe repay function,andEvefront-runsthattransactionwithherowncalltothe claim function.Asa result,EveisabletoliquidateAlice’sCryptoPunkcollateral. Recommendations Shortterm,introduceagraceperiodaftertheloan'smaturitydateduringwhichthelender cannotinvokethe claim function.Thisbufferwouldgivetheborrowersufficienttimeto repaytheloanwithouttheriskofimmediatecollateralliquidation.
Longterm,revisetheprotocol'sinterestassessmentdesigntoallowaportionofthe interesttoberefundedincasesofearlyrepayment.Thischangecouldreducetheincentive forborrowerstodelayrepaymentuntilthelastpossiblemoment.Additionally,provide bettereducationforborrowersonhowthelendingprotocolworks,particularlyaround

criticaldatesandactions,andimprovecommunicationchannelsforborrowerstoraise concernsorseekclarification. hasheye 50Arcade.xyzV3SecurityAssessment PUBLIC

14.itemPredicatesencodedincorrectlyaccordingtoEIP-712 Severity:LowDifficulty:Low Type:ConfigurationFindingID:TOB-ARCADE-14 Target: contracts/OriginationController.sol Description The itemPredicates parameterisnotencodedcorrectly,sothesignercannotseethe verifieraddresswhensigning.Theverifieraddressreceiveseachbatchoflistedassetsto checkthemforcorrectnessandexistence,whichisvitaltoensuringthesecurityand integrityofthelendingtransaction. AccordingtoEIP-712,structureddatashouldbehashedinconjunctionwithits typeHash . Thefollowingisthe hashStruct functionasdefinedinEIP-712: hashStruct(s:) =keccak256(typeHash ‖ encodeData(s)) wheretypeHash=keccak256(encodeType(typeOf(s))) Intheprotocol,therecoverItemsSignaturefunctionhashesanarrayofPredicate[] structsthatarepassedinasthe itemPredicates argument.Thefunctionencodesand hashesthearraywithoutaddingthe PredicatetypeHash toeachmemberofthearray. Thehashedoutputofthatoperationisthenincludedinthe _ITEMS_TYPEHASH variableas a bytes32 type,referredtoas itemsHash . 208(bytes32sighash,addressexternalSigner)=recoverItemsSignature(209loanTerms, 210sig, 211nonce, 212neededSide, 213keccak256(abi.encode(itemPredicates)) 214); Figure14.1:Asnippetofthe initializeLoanWithItems functionin arcade-protocol/contracts/OriginationController.sol 85bytes32privateconstant_ITEMS_TYPEHASH= 86keccak256(87//solhint-disablemax-line-length 88"LoanTermsWithItems(uint32durationSecs,uint32deadline,uint160 proratedInterestRate,uint256principal,addresscollateralAddress,bytes32 itemsHash,addresspayableCurrency,bytes32affiliateCode,uint160nonce,uint8side)" 89); hasheye 51Arcade.xyzV3SecurityAssessment PUBLIC

Figure14.2:The _ITEMS_TYPEHASH variablein arcade-protocol/contracts/OriginationController.sol However,thismethodofencodinganarrayofstructsisnotconsistentwiththeEIP-712 guidelines,whichstipulatesthefollowing: “Thearrayvaluesareencodedasthekeccak256hashoftheconcatenatedencodeDataof theircontents(i.e.,theencodingofSomeType[5]isidenticaltothatofastructcontaining fivemembersoftypeSomeType). ThestructvaluesareencodedrecursivelyashashStruct(value).Thisisundefinedfor cyclicaldata.” Therefore,theprotocolshoulditerateoverthe itemPredicates array,encodingeach Predicate instanceseparatelywithitsrespective typeHash . ExploitScenario AlicecreatesaloanofferingthattakesCryptoPunksascollateral.Shesubmitstheloan termstotheArcadeprotocol.Bob,aCryptoPunkholder,navigatestheArcadeUItoaccept Alice’sloanterms.AnEIP-712signaturerequestappearsinMetaMaskforBobtosign.Bob cannotvalidatewhetherthemessageheissigningusestheCryptoPunkverifiercontract becausethatinformationisnotincludedinthehash. Recommendations Shortterm,adjusttheencodingof itemPredicates tocomplywithEIP-712standards. Havethecodeiteratethroughthe itemPredicates arrayandencodeeach Predicate instanceseparatelywithitsassociated typeHash .Additionally,refactorthe _ITEMS_TYPEHASH variablesothatthe PredicatetypeHash definitionisappendedtoit andreplacethe bytes32itemsHash parameterwith Predicate[]items .Thisrevision willallowthesignertoseetheverifieraddressofthemessagetheyaresigning,ensuring thevalidityofeachbatchofitems,inadditiontocomplyingwiththeEIP-712standard. Longterm,strictlyadheretoestablishedEthereumprotocolssuchasEIP-712.These standardsexisttoensureinteroperability,security,andpredictablebehaviorinthe Ethereumecosystem.Violatingthesenormscanleadtounforeseensecurityvulnerabilities. hasheye 52Arcade.xyzV3SecurityAssessment PUBLIC

15.Thefeevaluescandistorttheincentivesfortheborrowersandlenders Severity:InformationalDifficulty:High Type:DataValidationFindingID:TOB-ARCADE-15 Target: contracts/FeeController.sol Description ArcadeV3containsninefeesettings.Sixofthesefeesaretobepaidbythelender,twoare tobepaidbytheborrower,andtheremainingfeeistobepaidbytheborrowerifthey decidetomintanewvaultfortheircollateral.Dependingonthevaluesofthesesettings, theincentivescanchangeforbothloancounterparties. Forexample,tocreateanewloan,boththeborrowerandlenderhavetopayorigination fees,andeventually,theloanmustberolledover,repaid,ordefaulted.Inthefirstcase, boththenewlenderandborrowerpayrolloverfees;notethattheoriginallenderpaysno feesatallforclosingtheloan.Inthesecondcase,thelenderpaysinterestfeesand principalfeesonclosingtheloan.Finally,iftheloanisdefaulted,thelenderpaysadefault feetoliquidatethecollateral. Thevariousfeespaidbasedontheoutcomeoftheloancanresultinaninteresting incentivegameforinvestorsintheprotocol,dependingontheactualvaluesofthefee settings.Ifthelenderrolloverfeeischeaperthantheoriginationfee,investorsmaybe incentivizedtorolloverexistingloansinsteadofcreatingnewones,benefitingtheoriginal

lendersbysavingthemtheclosingfees,andharmingtheborrowersbyindirectlyraising theinterestratestocompensate.Similarly,ifthelenderrolloverfeesarehigherthanthe closingfees,lenderswillbelessincentivizedtorolloverloans. Insummary,havingsuchfinecontroloverpossiblefeesettingsintroduceshard-to-predict incentivesscenariosthatcanscareusersawayorcauseuserswhodonotaccountforfees toinadvertentlyloseprofits. Recommendations Shortterm,clearlyinformborrowersandlendersofalloftheexistingfeesandtheir currentvaluesatthemomentaloanisopened,aswellasthevariouspossibleoutcomes, includingtheexpectednetprofitsiftheloanisrepaid,rolledover,defaulted,orredeemed. Longterm,addinteractivewaysforuserstocalculatetheirexpectedprofits,suchasaloan simulator. hasheye 53Arcade.xyzV3SecurityAssessment PUBLIC

16.MaliciousborrowerscanuseforceRepaytogrieflenders Severity:MediumDifficulty:Low Type:DataValidationFindingID:TOB-ARCADE-16 Target: contracts/RepaymentController.sol Description Amaliciousborrowercangriefalenderbycallingthe forceRepay functioninsteadofthe repay function;doingsowouldallowtheborrowertopaylessingasfeesandrequirethe lendertoperformaseparatetransactiontoretrievetheirfunds(usingthe redeemNote function)andtopayaredeemfee. Atanytimeaftertheloanissetandbeforethelenderclaimsthecollateraliftheloanis pastitsduedate,theborrowerhastopaytheirfulldebtbackinordertorecovertheir assets.Fordoingso,therearetwofunctionsin RepaymentController : repay and forceRepay .Thedifferencebetweenthemisthatthelattertransfersthetokenstothe LoanCore contractinsteadofdirectlytothelender.Itismeanttoallowtheborrowerto paytheirobligationswhenthelendercannotreceivetokensforanyreason. Forthelendertogettheirtokensbackinthisscenario,theymustcallthe redeemNote functionin RepaymentController ,whichinturncalls LoanCore.redeemNote ,which transfersthetokenstoanaddresssetbythelenderinthecall. Becausetheborrowerisfreetodecidewhichfunctiontocalltorepaytheirdebt,theycan arbitrarilydecidetodosovia forceRepay ,obligatingthelendertosendatransaction(with itsassociatedgasfees)torecovertheirtokens.Additionally,dependingonthe configurationoftheprotocol,itispossiblethatthelenderhastopayanadditionalfee (LENDER_REDEEM_FEE)togetbacktheirowntokens,cuttingtheirprofitswithnochanceto optout. 126functionredeemNote(uint256loanId,addressto)externaloverride{ 127LoanLibrary.LoanDatamemorydata=loanCore.getLoan(loanId); 128(,uint256amountOwed)=loanCore.getNoteReceipt(loanId); 129 130if(data.state≠LoanLibrary.LoanState.Repaid)revert RC_InvalidState(data.state); 131addresslender=lenderNote.ownerOf(loanId); 132if(lender≠msg.sender)revertRC_OnlyLender(lender,msg.sender); 133 134uint256redeemFee= (amountOwed*feeController.get(FL_09))/ BASIS_POINTS_DENOMINATOR; hasheye 54Arcade.xyzV3SecurityAssessment PUBLIC

135 136loanCore.redeemNote(loanId,redeemFee,to); 137} Figure16.1:The redeemNote functionin arcade-protocol/contracts/RepaymentController.sol Notethat,fromtheperspectiveoftheborrower,itisactuallycheapertocall forceRepay than repay becauseofthegassavedbynottransferringthetokenstothelenderandnot burningoneofthepromissorynotes. ExploitScenario Bobhastopaybackhisloan,andhedecidestodosovia forceRepay tosavegasinthe transaction.Lucy,thelender,wantshertokensback.Sheisnowforcedtocall redeemNote togetthem.Inthistransaction,shelostthegasfeesthattheborrowerwouldhavepaidto sendthetokensdirectlytoher,andshehastopayanadditionalfee (LENDER_REDEEMER_FEE) ,causinghertoreceivelessvaluefromtheloanthanshe originallyexpected. Recommendations Shortterm,removetheincentive(thelowergascost)fortheborrowertocall forceRepay insteadof repay .Considertakingoneofthefollowingactions: ● Forcethelendertoalwayspulltheirfundsusingthe redeemNote function.Thiscan beachievedbyremovingthe repay functionandrequiringtheborrowertocall forceRepay . ● Removethe forceRepay functionandmodifythe repay functionsothatit transfersthefundstothelenderina try/catch statementandcreatesaredeem note(whichthelendercanexchangefortheirfundsusingthe redeemNote function) onlyifthattransferfails. Longterm,whendesigningasmartcontractprotocol,alwaysconsidertheincentivesfor eachpartytoperformactionsintheprotocol,andavoidmakinganactorpayforthe mistakesormaliciousnessofothers.Bythoroughlydocumentingtheincentivesstructure, flawscanbespottedandmitigatedbeforetheprotocolgoeslive. hasheye 55Arcade.xyzV3SecurityAssessment 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
56Arcade.xyzV3SecurityAssessment 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
57Arcade.xyzV3SecurityAssessment PUBLIC

B.CodeMaturityCategories
Thefollowingtablesdescribethecodematuritycategoriesandratingcriteriausedinthis document.
CodeMaturityCategories CategoryDescription
ArithmeticTheproperuseofmathematicaloperationsandsemantics
AuditingTheuseofeventauditingandloggingtosupportmonitoring Authentication/ AccessControls
Theuseofrobustaccesscontrolstohandleidentificationand
authorizationandtoensuresafeinteractionswiththesystem Complexity Management
Thepresenceofclearstructuresdesignedtomanagesystemcomplexity,
includingtheseparationofsystemlogicintoclearlydefinedfunctions
DecentralizationThepresenceofadecentralizedgovernancestructureformitigating
insiderthreatsandmanagingrisksposedbycontractupgrades
DocumentationThepresenceofcomprehensiveandreadablecodebasedocumentation Transaction OrderingRisks
Thesystem’sresistancetofront-runningattacks Low-Level Manipulation
Thejustifieduseofinlineassemblyandlow-levelcalls Testingand Verification
Thepresenceofrobusttestingprocedures(e.g.,unittests,integration
tests,andverificationmethods)andsufficienttestcoverage RatingCriteria RatingDescription
StrongNoissueswerefound,andthesystemexceedsindustrystandards.
SatisfactoryMinorissueswerefound,butthesystemiscompliantwithbestpractices.
ModerateSomeissuesthatmayaffectsystemsafetywerefound.
WeakManyissuesthataffectsystemsafetywerefound.
MissingArequiredcomponentismissing,significantlyaffectingsystemsafety. hasheye
58Arcade.xyzV3SecurityAssessment PUBLIC

NotApplicableThecategoryisnotapplicabletothisreview.
NotConsideredThecategorywasnotconsideredinthisreview. Further Investigation Required
Furtherinvestigationisrequiredtoreachameaningfulconclusion. hasheye
59Arcade.xyzV3SecurityAssessment PUBLIC

C.CodeQualityRecommendations
Thefollowingrecommendationsarenotassociatedwithspecificvulnerabilities.However,
theyenhancecodereadabilityandmaypreventtheintroductionofvulnerabilitiesinthe future. •
Makefeenamesmoreexplicitandaddgettersforeachfee.Thenamesusedfor thevariousfeevalues(e.g., FL_0x
)donotclearlydescribethefees.Readersofthe codewillhavetonavigatebetweenthecurrentcontractandthe
FeeLookups contracttodeterminethetypeofeachfee.Additionally,addingcustomgetter functionstothe
FeeController contract(e.g., getLenderFee())cansimplifythe systembyallowing FeeLookups
toberemovedfromtheinheritancechainofthe OriginationController , RepaymentController ,and
VaultFactory contracts. • Ensurethatverifiersfollowtheprovideddocumentation.Accordingtothe
_runPredicatesCheck() NatSpecdocumentation,thefunctionrevertsifaverifier returns false
.However,someoftheimplementedverifierscanreturn true or false

orinsteadrevert.Eventhoughthisdiscrepancyhasnodirectimpactonthe system,anexternalentityinteractingwithArcademaybeconfusedbygettingan IV_xxx errorwhentheyexpectedan OC_PredicateFailed error. • Ensurethatstructurenamesareuniquethroughoutthesystem.Therearetwo structuresnamed SignatureItem :onein ArtBlocksVerifier andtheotherin ItemsVerifier .Eventhoughtheyaredefinedindifferentnamespaces,itcanbe confusingtoidentifythembecausetheyhavedifferentmembers.Moreover,inthe providedtestsuite,theyarereferredtoas ArtBlocksItem and SignatureItem , respectively,makingitmoreconfusingforreaders. • Useautomaticallygeneratedgettersforpublicvariables. OriginationController definesthemappings allowedVerifiers , allowedCurrencies ,and allowedCollateral aspublic.TheSolidity compiler automaticallyaddsgettersforthesevariables,butmanualgetterswereaddedby theteam(isAllowedVerifier , isAllowedCurrency ,and isAllowedCollateral)withnoadditionalfunctionalityfromthedefaultgetters. • Ensurethatcommentsinthecodereflectthecode’sintendedbehavior.Here aretwoexamplesofoff-by-onecommentsin OriginationController : OriginationController.sol#L669 and OriginationController.sol#L673 . • Ensurethatcontractnamesmatchtheirfilenames.The verifiers/ItemsVerifier.sol filecontainsthe ArcadeItemsVerifier contract. hasheye 60Arcade.xyzV3SecurityAssessment PUBLIC

• Removevariablesthatareneverusedorareusedonlyonce.Forexample, id in ArcadeItemsVerifier.verifyPredicates() isusedonlyonceinthefunction body. • Avoidredefiningconstants. FL_01 in FeeLookups wasredefinedin VaultFactory . • Removeunneededorunreachablecode.Forexample,the else conditioninthe ArcadeItemsVerifier.verifyPredicates functioncanneverbereached because abi.decode willrevertforincorrect CollateralType enumvalues. hasheye 61Arcade.xyzV3SecurityAssessment PUBLIC

D.RiskswithApprovingNFTsforUseasCollateral TheArcadeprotocolaimstowhitelistNFTcontractstobeusedascollateraltobackloans. TheseNFTscouldintroduceproblemsthatcouldallowattackerstostealfundsorotherwise impedethecorrectfunctioningofthesystem.WerecommendthattheArcadeteam exercisecautioninapprovingNFTsforuseascollateraltoensurethatthesystemkeeps workingcorrectlyandthatnouserlosesaccesstofunds. FollowtheseguidelineswhenconsideringwhichNFTstoapprove: • Tokensshouldneverbeupgradeable.UpgradeableERC-721tokenscanintroduce substantialriskswhenusedascollateralinanNFTlendingprotocol.Therefore, smartcontractdeveloperssholdeitherpreventupgradeabletokensfrombeing usedascollateralorimplementrobustsafeguardsagainsttheassociatedrisks. Someoftheserisksincludethefollowing: ○ Unpredictabletokenlogicchanges:Becausethecontractownerora designatedadmincanalterthelogicofanupgradeabletoken,thetoken’s behaviorcouldchangeunpredictablyduringtheloanperiod.Thiscould affectthevalueofthecollateral,renderitworthless,orpreventitsreturn. ○ Centralizationandminimizedtrust:Upgradeablecontractsintroducean elementofcentralization,asthepowertoupgradethecontracttypicallylies withaspecificaddressoraddresses.Thiscouldbeariskinadecentralized environment,wheretheethosistominimizetrustinindividualparties.The contract'sownercould,maliciouslyorunintentionally,makeanupgradethat jeopardizesthetoken'sroleascollateral. ○ Complexityandpotentialbugs:Upgradeablecontractsaremorecomplex thantheirnon-upgradeablecounterparts.Thisaddedcomplexityincreases theriskofbugsandvulnerabilities,whichcouldbeexploitedtothedetriment ofArcade’slendingprotocolanditsusers. • Tokensshouldnothaveaself-destructcapability.Theself-destructfunction allowsacontracttobedestroyedbyitsowner,whichessentiallyremovesthe contract'sbytecodefromtheEthereumblockchain,makingitnonfunctional.Here aresomeoftherisksofusingself-destructibletokensascollateral: ○ Totallossofcollateral:IfanERC-721tokenusedascollateralhasa self-destructfunctionandthatfunctionisinvokedduringtheloan'slifecycle, thetokenwillberenderedworthless.Theborrowercoulddefaultontheir loanandthelenderwouldnotbeabletoclaimthecollateral,leadingtoa completeloss. hasheye 62Arcade.xyzV3SecurityAssessment PUBLIC

○ DamagetotheintegrityofArcade’slendingprotocol:Suchtokenscan underminetheintegrityofthelendingprotocol.Lenderswillbeunwillingto participateiftheybelievethatthecollateralcouldself-destruct,makingit harderfortheprotocoltoattractandretainusers. ○ Lackofrecourse:Intraditionalfinance,therearelegalprotectionsto preventthedestructionofassetsusedascollateral.Incontrast,inthe blockchainworld,thereisnowaytorecoveracontractonceithas self-destructed,makingitasignificantriskforlenders. •

Tokensshouldnotbepausable.A"pause"function,whenpresentinasmart contract,allowscertainprivilegedaccountssuchascontractownersand administratorstostopspecificactivitiessuchastokentransfersforaperiodoftime. Althoughthisfunctionalitycanbeusefulforhaltingactivitiesincaseofadetected vulnerabilityorbug,itcanposesignificantriskstoanNFTlendingprotocol,suchas thefollowing: ○ Possiblepreventionofrepaymentandcollateralretrieval:Ifatokenused ascollateralispaused,thattokencannotbetransferred.Thismeansthata borrowercouldnotrepaytheirloanandretrievetheircollateral,and similarly,alendercouldnotclaimthecollateraliftheloandefaults. ○ Marketmanipulation:Inaworst-casescenario,amaliciousstokenowner couldstrategicallypauseandunpauseatoken,disruptingthemarketand possiblymanipulatingthetoken’svalue. ● Tokensshouldnotbeburnablebysomeauthorizedthird-party.Tokensthatcan beburnedbyathird-partyortokenadminshouldnotbepermittedascollateralin anNFTlendingprotocol.“Burning”isaprocessbywhichtokensarepermanently removedfromcirculation,therebyreducingthetotalsupplyoftokens.Althoughthis featurecanbeusefulincertaincontexts,itcanintroducethefollowingriskswhen usedinanNFTlendingprotocol: ○ Totallossofcollateral:Ifthetokenusedascollateralcanbeburnedbyan adminorthirdparty,itcouldbeburnedduringthedurationoftheloan, whichwouldleavethelenderunprotectedinthecaseofadefault. ○ Loan-to-valuemanipulation:Thosewiththeabilitytoburntokenscould engageinmanipulativebehaviorsthatdisrupttheloan-to-valueratio,suchas artificiallyinfluencingatoken’sscarcityandtherebyitsmarketvalue,thus leadingtoover-collateralizationorunder-collateralization. ● Tokensshouldnotholdorhaveaccesstootherassets.Tokenscanbestructured toholdorinteractwithotherassetsontheblockchain.AnERC-721tokencanbea hasheye 63Arcade.xyzV3SecurityAssessment PUBLIC

"wrapper"forspecificERC-20tokens,generateyieldsfromaDeFiprotocol,or representin-gamecharacterswiththeirownassets.Usingthemascollateralin lendingprotocolcomeswiththefollowingrisks: ○ Valuefluctuation:Ifthetokenholdsorhasaccesstootherassets,itsvalue canchangeduringtheloanperiodifthevalueoftheunderlyingassets changes.Ifacollateralchangesvalue,itmaynolongercoverthevalueofthe loan,creatingsignificantriskforthelender. ○ Assetremovaloraddition:Ifthetokenallowsassetstobeaddedtoor removedfromit,thevalueofthecollateralcouldbealteredduringthelife cycleoftheloan.Aborrowerorathirdpartycouldremoveassetsfromthe collateral,decreasingthecollateral’svalue;thelenderandtheprotocolwould havenomeanstopreventthis. ○ Valuationcomplexity:Valuingtokensthatholdotherassetsismore complexthanvaluingsimplertokens.Someassetsareinterestbearing,some undergorebasing,andmostaretradedonpublicmarkets.Thecomplexities involvedinaccuratelydeterminingthevalueofsuchtokensintroduces additionalrisksandcomplexitiesforthelender,theborrower,andthe protocolingeneral. ● Gamingtokenswithalterableintrinsicvalueshouldbeavoided.Tokensare oftenusedtorepresentuniquedigitalassetsingamingenvironments,suchas characters,equipment,andvirtualrealestate.Usingthemascollateralinalending protocolcarriessomerisks,suchasthefollowing: ○ Developercontrol:Gamedevelopersoftenmaintainadegreeofcontrol overin-gameassets,whichmayincludetheabilitytocreate,modify,or destroyassets.Ifagamedeveloperdecidestofloodthemarketwithcopies ofapreviouslyrareasset,oralteritscapabilitieswithinthegame,thevalue ofthecollateralcouldbesignificantlyaffected. ○ In-gamerulesandactions:In-gameactionsbyotherplayersorchangesto in-gamerulescaninfluencethevalueofthetoken.Forinstance,ifthegame involvesplayercompetition,otherplayers’actionscoulddiminishthevalue ofthecollateraltoken. hasheye 64Arcade.xyzV3SecurityAssessment PUBLIC

E.TokenIntegrationChecklist Thefollowingchecklistprovidesrecommendationsforinteractionswitharbitrarytokens. Everyuncheckeditemshouldbejustified,anditsassociatedrisks,understood.Foran up-to-dateversionofthechecklist,see crytic/building-secure-contracts . Forconvenience,allSlitherutilitiescanberundirectlyonatokenaddress,suchasthe following: slither-check-erc0xdac17f958d2ee523a2206206994597c13d831ec7TetherToken--ercerc20 slither-check-erc0x06012c8cf97BEaD5deAe237070F9587f8E7A266dKittyCore--ercerc721 Tofollowthischecklist,usethebelowoutputfromSlitherforthetoken: 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 adviseusers(likeyou!)whencriticalissuesarefoundorwhenupgradesoccur. ContractComposition
▯Thecontractavoidsunnecessarycomplexity.Thetokenshouldbeasimple contract;atokenwithcomplexcoderequiresahigherstandardofreview.Use Slither's human-summary printertoidentifycomplexcode. ▯Thecontractuses SafeMath .Contractsthatdonotuse SafeMath requireahigher standardofreview.Inspectthecontractbyhandfor SafeMath usage.
▯Thecontracthasonlyafewnon-token-relatedfunctions.Non-token-related functionsincreasethelikelihoodofanissueinthecontract.UseSlither's contract-summary printertobroadlyreviewthecodeusedinthecontract. hasheye 65Arcade.xyzV3SecurityAssessment PUBLIC

▯Thetokenhasonlyoneaddress.Tokenswithmultipleentrypointsforbalance updatescanbreakinternalbookkeepingbasedontheaddress(e.g., balances[token_address][msg.sender] maynotreflecttheactualbalance). OwnerPrivileges
▯Thetokenisnotupgradeable.Upgradeablecontractsmaychangetheirrulesover time.UseSlither's human-summary printertodeterminewhetherthecontractis upgradeable.
▯Theownerhaslimitedmintingcapabilities.Maliciousorcompromisedowners canabusemintingcapabilities.UseSlither's human-summary printertoreview mintingcapabilities,andconsidermanuallyreviewingthecode.
▯Thetokenisnotpausable.Maliciousorcompromisedownerscantrapcontracts relyingonpausabletokens.Identifypausablecodebyhand.
▯Theownercannotblacklistthecontract.Maliciousorcompromisedownerscan trapcontractsrelyingontokenswithablacklist.Identifyblacklistingfeaturesby hand.
▯Theteambehindthetokenisknownandcanbeheldresponsibleforabuse. Contractswithanonymousdevelopmentteamsorteamsthatresideinlegalshelters requireahigherstandardofreview. ERC20Tokens ERC20ConformityChecks 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 areoptionalintheERC20standardandmaynotbepresent. ▯ Decimals returnsa uint8 .Severaltokensincorrectlyreturna uint256 .Insuch cases,ensurethatthevaluereturnedisbelow255.
▯ThetokenmitigatestheknownERC20racecondition.TheERC20standardhasa knownERC20raceconditionthatmustbemitigatedtopreventattackersfrom stealingtokens. Slitherincludesautility, slither-prop ,thatgeneratesunittestsandsecurityproperties thatcandiscovermanycommonERCflaws.Use slither-prop toreviewthefollowing: hasheye 66Arcade.xyzV3SecurityAssessment PUBLIC

▯Thecontractpassesallunittestsandsecuritypropertiesfrom slither-prop . Runthegeneratedunittestsandthencheckthepropertieswithechidnaand Manticore. RisksofERC20Extensions Thebehaviorofcertaincontractsmaydifferfromtheoriginal ERCspecification.Conducta manualreviewofthefollowingconditions: ▯ThetokenisnotanERC777tokenandhasnoexternalfunctioncallin transfer or transferFrom .Externalcallsinthetransferfunctionscanleadto reentrancies. ▯ Transfer and transferFrom shouldnottakeafee.Deflationarytokenscanlead tounexpectedbehavior.
▯Potentialinterestearnedfromthetokenistakenintoaccount.Sometokens distributeinteresttotokenholders.Thisinterestmaybetrappedinthecontractif nottakenintoaccount. TokenScarcity Reviewsoftokenscarcityissuesmustbeexecutedmanually.Checkforthefollowing conditions:
▯Thesupplyisownedbymorethanafewusers.Ifafewusersownmostofthe tokens,theycaninfluenceoperationsbasedonthetokens'repartition.
▯Thetotalsupplyissufficient.Tokenswithalowtotalsupplycanbeeasily manipulated.
▯Thetokensarelocatedinmorethanafewexchanges.Ifallthetokensareinone exchange,acompromiseoftheexchangecouldcompromisethecontractrelyingon thetoken.
▯Usersunderstandtherisksassociatedwithalargeamountoffundsorflash loans.Contractsrelyingonthetokenbalancemustaccountforattackerswitha largeamountoffundsorattacksexecutedthroughflashloans.
▯Thetokendoesnotallowflashminting.Flashmintingcanleadtosubstantial swingsinthebalanceandthetotalsupply,whichnecessitatestrictand comprehensiveoverflowchecksintheoperationofthetoken. hasheye 67Arcade.xyzV3SecurityAssessment PUBLIC

ERC721Tokens ERC721ConformityChecks
Thebehaviorofcertaincontractsmaydifferfromtheoriginal ERCspecification.Conducta manualreviewofthefollowingconditions: ▯Transfersoftokenstothe 0x0 addressrevert.Severaltokensallowtransfersto 0x0 andconsidertokenstransferredtothataddresstohavebeenburned;however, theERC721standardrequiresthatsuchtransfersrevert. ▯ safeTransferFrom functionsareimplementedwiththecorrectsignature. Severaltokencontractsdonotimplementthesefunctions.AtransferofNFTstoone ofthosecontractscanresultinalossofassets. ▯The name , decimals ,and symbol functionsarepresentifused.Thesefunctions areoptionalintheERC721standardandmaynotbepresent. ▯Ifitisused,the decimals functionreturnsa uint8(0) .Othervaluesareinvalid. ▯The name and symbol functionscanreturnanemptystring.Thisbehavioris allowedbythestandard. ▯The ownerOf functionrevertsifthe tokenId isinvalidorissettoatokenthat hasalreadybeenburned.Thefunctioncannotreturn 0x0 .Thisbehavioris requiredbythestandard,butitisnotalwaysproperlyimplemented. ▯AtransferofanNFTclearsitsapprovals.Thisisrequiredbythestandard. ▯ThetokenIDofanNFTcannotbechangedduringitslifetime.Thisisrequired bythestandard.
CommonRisksoftheERC721Standard
TomitigateterisksassociatedwithERC721contracts,conductamanualreviewofthe followingconditions: ▯The onERC721Received callbackistakenintoaccount.Externalcallsinthe transferfunctionscanleadtoreentrancies,especiallywhenthecallbackisnot explicit(e.g.,in safeMint calls). hasheye 68Arcade.xyzV3SecurityAssessment PUBLIC

▯WhenanNFTisminted,itissafelytransferredtoasmartcontract.Ifthereisa mintingfunction,itshouldbehavesimilarlyto safeTransferFrom andproperly handlethemintingofnewtokenstoasmartcontract.Thiswillpreventalossof assets. ▯Theburningofatokenclearsitsapprovals.Ifthereisaburningfunction,it shouldclearthetoken’s previousapprovals hasheye 69Arcade.xyzV3SecurityAssessment PUBLIC

F.MutationTesting Thegoalofmutationtestingistogaininsightintoacodebase’stestcoverage.Mutation testsgoline-by-linethroughthetargetfile,mutatethegivenlineinsomeway,runtests, andflagchangesthatdonottriggertestfailures.Dependingonthecomplexityofthelogic inanygivenlineandthetoolusedtomutate,mutationtestscouldtestupwardsof50 mutantsperlineofsourcecode.Mutationtestingisaslowprocess,butbyhighlighting areasofthecodewithincompletetestcoverage,itallowsauditorstofocustheirmanual reviewonthepartsofthecodethataremostlikelytocontainlatentbugs. Inthissection,weprovideinformationonavailablemutationtestingtoolsthatcouldbe usedintheArcadeV3codebase,andwedescribethemutationtestingcampaignthatwe conducteduringthisaudit. Thefollowingareavailablemutationtestingtools: • Universalmutator:Thistoolgeneratesdeterministicmutantsfromregular expressions;itsupportsmanysourcecodelanguages,includingSolidityandVyper. Refertothe2018ICSEpaperonthetoolandthisguestblogpostaboutthetoolon thehasheyeblogformoreinformation. • Necessist:Thistoolwasdevelopedin-housebyhasheye.Itoperatesontests ratherthansourcecode,althoughithasasimilarendgoal.Necessistcouldprovide anicecomplementtosource-focusedmutationtesting.Duetothetime-boxed natureofthisreview,wedeprioritizedtheuseofNecessisttoconductanadditional mutationtestingcampaign. • Vertigo:Thistoolwasdevelopedbysecurityresearchersat ConsensysDiligence. IntegrationwithFoundryisplanned,butthecurrentprogressonthatworkis unclear.Knownscalabilityissuesarepresentinthetool. • Gambit:ThistoolgeneratesstochasticmutantsbymodifyingtheSolidityAST.Itis optimizedforintegrationwiththeCertoraprover. Weuseduniversalmutatortoconductamutationtestingcampaignduringthisengagement becausethemutantsitgeneratesaredeterministicandbecauseitisarelativelymature toolwithfewknownissues.Thistoolcanbeinstalledwiththefollowingcommand: pipinstalluniversalmutator
FigureF.1:Thecommandusedtoinstalluniversalmutator
Onceinstalled,amutationcampaigncanberunagainstallSolidityfilesusingthe followingbashscript: hasheye 70Arcade.xyzV3SecurityAssessment PUBLIC

```
1findcontracts\ 2-name'*.sol'\ 3-not-path'*/interfaces/*'\ 4-not-path'*/test/*'\ 5-not-path'*/external/*'\ 6-print0|whileIFS=read-r-d''file 7do 8name="$(basename"$file".sol)" 9dir="mutants/$name" 10mkdir-p"$dir" 11echo"Mutating$file" 12mutate"$file"\ 13--cmd"timeout200snpxhardhattest"\ 14--mutantDir"$dir"\ 15>"mutants/$name.log" 16done
```

FigureF.2:AbashscriptthatrunsamutationtestingcampaignagainsteachSolidityfileinthe contracts directory Considerthefollowingnotesabouttheabovebashscript: • Theoverallruntimeoftheabovescriptagainstallnon-excludedSolidityfilesinthe target contracts

repositoryisapproximatelyoneweekonamodernM2Mac.This executiontimeisdirectlyrelatedtothe npxhardhattest toolruntimeandthe numberofcontractstobemutated. ● The --cmd argumentonline13specifiesthecommandtorunforeachmutant.This commandisprefixedby timeout200s (timeout isatoolincludedinthe coreutils packageonmacOS)becauseahealthyrunofthetestsuitewas measuredtotakeapproximately150seconds.Atimeoutlongerthantheaverage testsuiteruntimeisusedonlytocutofftestrunsthatarebadlystalled. Theresultsofeachtarget'smutationtestsaresavedinafile,perline15ofthescriptin figureF.2.Anillustrativeexampleofsuchoutputisshowninfigure F.3. ***UNIVERSALMUTATOR*** MUTATINGWITHRULES:audit-arcade/custom-solidity.rules FAILEDTOFINDRULEaudit-arcade/custom-solidity.rulesASBUILT-IN... SKIPPED458MUTANTSONLYCHANGINGSTRINGLITERALS 2761MUTANTSGENERATEDBYRULES ... PROCESSINGMUTANT:121:if(_feeController==address(0))revert OC_ZeroAddress();⟹if(_feeController≠address(0))revert OC_ZeroAddress();...INVALID PROCESSINGMUTANT:121:if(_feeController==address(0))revert OC_ZeroAddress();⟹if(_feeController⩽address(0))revert OC_ZeroAddress();...VALID[writtento mutants/OriginationController/OriginationController.mutant.25.sol] hasheye

PROCESSINGMUTANT:121:if(_feeController==address(0))revert OC_ZeroAddress();⟹if(_feeController⩾address(0))revert OC_ZeroAddress();...INVALID ... PROCESSINGMUTANT:375:)publicoverridereturns(uint256newLoanId){⟹)publicoverridereturns(uint256{...INVALID PROCESSINGMUTANT:375:)publicoverridereturns(uint256newLoanId){⟹)publicoverridereturns(uint256newLoanId)...INVALID PROCESSINGMUTANT:375:_validateLoanTerms(loanTerms);⟹ /*_validateLoanTerms(loanTerms);*/...VALID[writtento mutants/OriginationController/OriginationController.mutant.46.sol] PROCESSINGMUTANT:375:_validateLoanTerms(loanTerms);⟹ selfdestruct(msg.sender);...INVALID PROCESSINGMUTANT:375:_validateLoanTerms(loanTerms);⟹ revert();...INVALID ... 156VALIDMUTANTS 2605INVALIDMUTANTS 0REDUNDANTMUTANTS ValidPercentage:5.650126765664615% FigureF.3:Abbreviatedoutputfromthemutationtestingcampaignon OriginationController.sol Theoutputofuniversalmutatorstartswiththenumberofmutantsgeneratedandends withasummaryofhowmanyofthesemutantsarevalid.Asmallpercentageofvalid mutantsindicatesthoroughtestcoverage. Thefirsthighlightedsnippetinthemiddleoftheoutputisfocusedonmutationsmadeto line121ofthe OriginationController sourcecode.Thisparticularlineshowsa mutationwithafalsepositive:thismeansthatwhilethemutantcompilesandpassesall tests,themutationdoesnotimplyfailureintestcoveragebecausetheaddresscannotbe negative.Othertypesofcommonfalsepositivesincluderemovingthepublicvisibility modifierfromvariableorfunctiondeclarations. However,thesecondhighlightedsnippetshowsthatcommentingoutline375ofthe OriginationController sourcecodemakesthetestrunsucceed.Becausethischange canhaveconsequencesintheresultsofthefunction,thismutantisexpectedtobeinvalid giventhoroughtestcoverage.Inthatparticularcase,itmeansthatnoneofthe implementedtestsforthe OriginationController contracttriestorolloveraloanwith invalidloanterms.Forauditors,thisisacuetotakeanextracloselookatthe implementationofthismethodandatitsusethroughouttherestofthecodebase. Werecommendrunningmutationtestsonthecodeeverytimemajorchangesaremadeto thecodeortothetestsuite,andwerecommendfilteringtheresultstoensurethatthetest coverageiscorrect.

G.IncidentResponsePlanRecommendations

Thissectionprovidesrecommendationsonformulatinganincidentresponseplan. ● Identifytheparties(eitherspecificpeopleorroles)responsiblefor implementingthemitigationswhenanissueoccurs(e.g.,deployingsmart contracts,pausingcontracts,upgradingthefrontend,etc.). ● Clearlydescribetheintendedcontractdeploymentprocess. ● Outlinethecircumstancesunderwhichthe Arcadeprotocolwillcompensate usersaffectedbyanissue(ifany). ○ Issuesthatwarrantcompensationcouldincludeanindividualoraggregate lossoralossresultingfromusererror,acontractflaw,orathird-party contractflaw. ● Documenthowtheteamplanstostayuptodateonnewissuesthatcould affectthesystem;awarenessofsuchissueswillinformfuturedevelopment workandhelptheteamsecurethedeploymenttoolchainandtheexternal on-chainandoff-chainservicesthatthesystemrelieson. ○ Identifysourcesofvulnerabilitynewsforeachlanguageandcomponentused inthesystem,andsubscribetoupdatesfromeachsource.Considercreating

aprivateDiscordchannelinwhichabotwillpostthelatestvulnerability news;thiswillprovidetheteamwithawaytotrackallupdatesinoneplace. Lastly,considerassigningcertainteammemberstotracknewsabout vulnerabilitiesinspecificcomponentsofthesystem. • Determinewhentheteamwillseekassistancefromexternalparties(e.g., auditors,affectedusers,otherprotocoldevelopers,etc.)andhowitwill onboardthem. ○ Effectiveremediationofcertainissuesmayrequirecollaborationwith externalparties. • Definecontractbehaviorthatwouldbeconsideredabnormalbyoff-chain monitoringsolutions. Itisbestpracticetoperformperiodicdryrunsofscenariosoutlinedintheincident responseplantofindomissionsandopportunitiesforimprovementandtodevelop “musclememory.”Additionally,documentthefrequencywithwhichtheteamshould performdryrunsofvariousscenarios,andperformdryrunsofmorelikelyscenariosmore hasheye 73Arcade.xyzV3SecurityAssessment PUBLIC

regularly.Createatemplatetobefilledoutwithdescriptionsofanynecessary improvementsaftereachdryrun. hasheye 74Arcade.xyzV3SecurityAssessment PUBLIC

H.FixReviewResults Whenundertakingafixreview,hasheyereviewsthefixesimplementedforissues identifiedintheoriginalreport.Thisworkinvolvesareviewofspecificareasofthesource codeandsystemconfiguration,notcomprehensiveanalysisofthesystem. OnJuly24toJuly25,2023,hasheyereviewedthefixesandmitigationsimplementedby theArcadeteamfortheissuesidentifiedinthisreport.Wereviewedeachfixtodetermine itseffectivenessinresolvingtheassociatedissue. Insummary,ofthe16issuesdescribedinthisreport,Arcadehasresolved12issuesand hasnotresolvedtheremainingfourissues.Foradditionalinformation,pleaseseethe DetailedFixReviewResultsbelow. IDTitleSeverityStatus 1Differentzero-addresserrorsthrownbysingleand batchNFTwithdrawalfunctions InformationalResolved 2SolidityCompileroptimizationscanbeproblematicUndeterminedUnresolved 3callApprovedoesnotfollowapprovalbest practices InformationalResolved 4Riskofconfusingeventsduetomissingchecksin whitelistcontracts LowResolved 5Missingchecksof_exists()returnvalueInformationalResolved 6IncorrectdeployersinintegrationtestsInformationalResolved 7Riskofout-of-gasrevertduetouseoftransfer()in claimFees InformationalResolved 8Riskoflostfundsduetolackofzero-addresscheck infunctions MediumResolved hasheye 75Arcade.xyzV3SecurityAssessment PUBLIC

9ThemaximumvalueforFL_09isnotsetby FeeController LowResolved 10FeescanbechangedwhilealoanisactiveLowResolved 11AssetvaultnestingcanleadtolossofassetsLowUnresolved 12Riskoflockedassetsduetouseof_mintinsteadof _safeMint MediumResolved 13Borrowerscannotrealizefullloanvaluewithout riskingdefault MediumResolved 14itemPredicatesencodedincorrectlyaccordingto EIP-712 LowResolved 15Thefeevaluescandistorttheincentivesforthe borrowersandlenders InformationalUnresolved 16MaliciousborrowerscanuseforceRepaytogrief lenders MediumUnresolved DetailedFixReviewResults TOB-ARCADE-1:Differentzero-addresserrorsthrownbysingleandbatchNFT withdrawalfunctions Resolvedincommits 00e8130 and 8542c46 .The AV_ZeroAddress errorwasupdatedto includea stringaddressType argumentthatisusedtoindicatewhichaddress parameterviolatedazero-addresscheckrequirement.Additionalzero-addresschecks wereaddedtofunctionsinthe AssetVault contract,unittestswereimplementedto ensurethatthesechecksworkasexpected,andtheNatSpeccommentswereupdatedto reflectthisupdate. TOB-ARCADE-2:SolidityCompileroptimizationscanbeproblematic Unresolved.Arcadeprovidedthefollowingstatementaboutthisissue: TheArcadeteamunderstandsthatSolidityCompileroptimizationsmaypotentiallybe problematic.Howevertoremoveourcompileroptimizationwewouldneedtodownsize fourofoursmartcontractsinextensiveways,breakingthemupintosmallercontracts andconsiderablyincreasingourcodefootprint,introducingmorecomplexityand possiblynewrisks. hasheye 76Arcade.xyzV3SecurityAssessment PUBLIC

Weelectednottodothisatthistime,giventhattheexistenceofavulnerabilityremains undetermined.Beforethenextmajorprotocolrelease,theArcadeteamwillrevisitthis issue. TOB-ARCADE-3:callApprovedoesnotfollowapprovalbestpractices Resolvedincommits a3ce932 and 77c1db0 .The AssetVault contractnowincludestwo newfunctions, callIncreaseAllowance and callDecreaseAllowance ,whichenable safeinteractionswithArcadeforthird-partyintegrations.The callApprove functionwas temporarilyremovedincommit a3ce932 butwassubsequentlyaddedbackincommit 77c1db0 .Toaidthird-partyintegratorsandtesttheexpectedfunctionalityofthenewly addedfunctions,documentationandunittestshavebeenaddedappropriately. TOB-ARCADE-4:Riskofconfusingeventsduetomissingchecksinwhitelistcontracts Resolvedincommit 2434705 .Twonewerrortypes, CW_AlreadyWhitelisted and CW_NotWhitelisted

,havebeenaddedandimplementedforwhitelistingfunctions.Ifthe addresshasalreadybeenaddedortheaddresstargetedforremovalisnotfound,the whitelistingfunctionswillnowrevert.NatSpeccommentshavebeenaddedtodescribe eacherror,andunittestshavebeenincludedtotestthe add and remove functionsforthe expectedrevert. TOB-ARCADE-5:Missingchecksof_exists()returnvalue Resolvedincommit e04502b .Newreasonsfor DoesNotExist revertswereaddedtothe Lending and Vault contracts.The VaultFactory and PromissoryNote contractsnow usetheserevertreasonsinthe tokenURI functionswhentherequested tokenId is nonexistent. Additionally,newtestswereimplementedfor VaultFactory and PromissoryNote that checkfortheexpectedrevertreasonwhenanonexistent tokenId isused. TOB-ARCADE-6:Incorrectdeployersinintegrationtests Resolvedincommit dddc905 .Theincorrectdeployersinintegrationtestcaseswere changedfrom signers[0] to admin .Anewtestwasimplementedtocheckthatthe correctpermissionsaresetwhentheprotocolisdeployed. TOB-ARCADE-7:Riskofout-of-gasrevertduetouseoftransfer()inclaimFees Resolvedincommit a948cfc .Commentswereaddedtoinformusersanddevelopers abouttheissue,butnofurtherchangesweremadetothecontract. TOB-ARCADE-8:Riskoflostfundsduetolackofzero-addresscheckinfunctions Resolvedincommit a6dbd53 .Existingerrortypesrelatedto ZeroAddress weremodified toincludeastringparameterindicatingtheaddressthatfailedthezero-addresscheck(also refertothefixstatusforissueTOB-ARCADE-1).Theusesoftheolderrortypewithno argumentswerereplacedwiththenewversion. hasheye 77Arcade.xyzV3SecurityAssessment PUBLIC

Newzero-addresschecksforthetokenanddestinationaddresseswereimplementedin the LoanCore.withdraw and LoanCore.withdrawProtocolFees functions.Checksfor thedestinationaddresswereaddedtothe RepaymentController.redeemNote and VaultFactory.claimFees functions. Existingtestsweremodifiedtoaccountforthenewstringparameterinerrortypes,and newtestswereimplementedforzero-addressparametersinthefixedfunctions. TOB-ARCADE-9:ThemaximumvalueforFL_09isnotsetbyFeeController Resolvedincommit a51dfd8 .Thevalueof maxFees[FL_09] isnowsetproperlyinthe constructorofthe FeeController contract.Theunittestsuitehasalsobeenexpandedto includeteststhatensurethatallmaximumfeevaluesareproperlyset. TOB-ARCADE-10:Feescanbechangedwhilealoanisactive Resolvedincommit f7b87a7 .Thefiximplementedforthisissueconsistsofseveralparts. Feenameswerechanged.Previously,the FeeLookups constantsrangedfrom FL_01 to FL_09 ,where FL_01 wasthevaultmintingfeeand FL_02 to FL_09 werethedifferentfees thattheborrowersandlendersshouldpayforaloan.TheArcadeteamrenamed FL_02 through FL_09 to FL_01 through FL_08 andremovedtheformer FL_01 from FeeLookups andreplaceditwith vaultMintFee in FeeController . Thefunctionsforsettingandgettingthefeeswererenamedto setLendingFee and getLendingFee ,respectively.Thenew getFeesOrigination and getFeesRollover functionswereaddedtosimplifytheprocessofretrievingthefeesfortheloanorigination androlloverprocesses. Anew FeeSnapshot structurewascreatedtotakeasnapshotofthefeevaluesatthe momentaloanisoriginatedtoensurethatfuturechangestofeesdonotaffectexisting loans.However,onlythevaluesforthedefault,interest,andprincipalfees(fees FL_05 through FL_07)arestored,andtheredeemfee(FL_08)isreadfrom feeController at themomentofredeeming.Eventhoughthisfeelscounterintuitive,itisconsistentwiththe statementgivenbyArcadeforthefixstatusoffindingTOB-ARCADE-16;havingtheredeem feereadfrom feeController allowsprotocoladminstochangethefeetoprevent griefing. Existingtestsweremodifiedtocomplywiththenewchanges.Newtestswereaddedin RepaymentController and feeController . TOB-ARCADE-11:Assetvaultnestingcanleadtolossofassets Unresolved.Arcadeprovidedthefollowingstatementaboutthisissue: TheArcadeteamunderstandsthelikelihoodofthisproblemoccurringisquitelow becauseourUIdoesnotallowforvaultkeys(vaulttrackingERC721tokens)tobe hasheye 78Arcade.xyzV3SecurityAssessment PUBLIC

depositedinsideanothervaultcontract.Apoweruserwouldneedtoexecutethistypeof vaultkeytransferviaEtherscan. Weelecttoaddressthisissueby: • Thoroughlydocumentingthisriskandprovidingclearandcomprehensive warningsagainstthisspecificactioninthedocumentation • Maintainingouruserinterfacetoensurethatitdoesnotpresentthe optionof usingvaultkeysascollateralforloans TOB-ARCADE-12:Riskoflockedassetsduetouseof_mintinsteadof_safeMint Resolvedincommit 20b7c66 .The mint functioninthe PromissoryNote contracthas beenupdatedtouse _safeMint insteadof _mint .Similarly,the initializeBundle functioninthe VaultFactory contractnowuses _safeMint insteadof _mint .These changesensurethatanERC-721tokenisnotsenttoacontractaddressthatisnot configuredtoreceiveit.TheNatSpeccommentshavealsobeenupdatedtoreflectthese changes.Additionally,theunittestingsuiteandmockcontractshavebeenupdatedto adequatelytestthenewexpectedbehaviorofthetwoalteredfunctions. TOB-ARCADE-

13:Borrowerscannotrealizefullloanvaluewithoutriskingdefault Resolvedincommits 6586c37 and f1eb8ae .Anewgraceperiodaftertheoriginalloan’s duedatewasintroducedwiththefirstcommit.Thegraceperiodaddedinthiscommitwas aconfigurablesettingthatcanbebetweenonehourandsevendays.Anadmin-only functionwasaddedtosetthenewvalue,whichemitseventsonchangesorerrors.Anew setofunittestswasaddedforthe setGracePeriod functionality,andexistingtestswere modifiedtotakethegraceperiodintoaccount. However,inthesecondcommit,thevariablegraceperiodwasreplacedwithaconstant 10-minuteperiod.Thevariableperiodtestswereremoved,andtheremainingtestswere modifiedtoaccountforthechange. TOB-ARCADE-14:itemPredicatesencodedincorrectlyaccordingtoEIP-712 Resolvedincommit c95e21c .Itempredicatesarenowencodedincompliancewiththe EIP-712standard.Ratherthanahashrepresentinganarrayofitempredicates,anarrayof theactual Predicate structstobesignedisnowpresentedtothesigner.A _PREDICATE_TYPEHASH hasbeencreated,andthe _ITEMS_TYPEHASH hasbeenupdated tocorrectlyaccountforthearrayof Predicate structsthatisnowrepresentedinthe signature.Theunittestsdealingwithsignaturesthatincludeitemshavebeenupdatedto reflectthechangestothesignaturescheme. TOB-ARCADE-15:Thefeevaluescandistorttheincentivesfortheborrowersand lenders Unresolved.Arcadeprovidedthefollowingstatementaboutthisissue: hasheye 79Arcade.xyzV3SecurityAssessment PUBLIC

OurV3documentationwillcomprehensivelyoutlineallfeeswithinthelendingprotocol, pointingtheuserstotheirvaluesatloaninitiation.TheArcadeteam’sobjectiveistohelp usersgrasppotentialprofitsandanticipatedfeeslinkedwithloanrepayment,rollover, default,orredemptionscenarios. TOB-ARCADE-16:MaliciousborrowerscanuseforceRepaytogrieflenders Unresolved.Arcadeprovidedthefollowingstatementaboutthisissue: TheArcade.xyzteamisawarethatforhonestlenders,havingforceRepaycalledincurs additionalgascostandpossiblefees.Nevertheless,theteamhaselectedtokeepthe implementationas-is:wefeelthathavingtwoseparatefunctionsisamoreexplicit,less "surprising"designcomparedtohavingasinglefunctionwhoseeffectsmaychange basedonexternalstate. Ingeneral,webelievethevectorallowingborrowergriefingisbestmitigatedthrough properincentivemanagementandcounterpartyrelationshipmanagement:borrowers whohavegriefedlendersinthepastarelikelytoreceivelendingofferswithhigher premiums,aslenderstrytomitigatetheirrisk.Inalargersense,ifgriefingbecomesa protocol-wideissue,redeemfeescanbesetto0. hasheye 80Arcade.xyzV3SecurityAssessment PUBLIC