HashEye

// SMART CONTRACT SECURITY AUDIT

Offchain Stylus

Security assessment by HashEye · prepared for Offchain Labs

HASHEYE AUDITED

PROJECT	Offchain Stylus
CLIENT	Offchain Labs
CATEGORY	Offchain Labs
PUBLISHED	September 1, 2024
REPORT ID	research-offchain-stylus-2024-09-01-75kgut

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-offchain-stylus-2024-09-01-75kgut.

StylusEmergencyFixesReview SecurityAssessment(SummaryReport) October23,2024 Preparedfor: OffchainLabs Preparedby:GustavoGriecoandJaimeIglesias

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

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

TableofContents Abouthasheye1 NoticesandRemarks2 TableofContents3 ProjectSummary4 ProjectTargets5 ExecutiveSummary6 SummaryofFindings7 DetailedFindings8 1.Importingforward__set_trapproducesafailureinWASMinstantiation8 A.VulnerabilityCategories10 B.CodeQualityRecommendations12 General12 arbitrator/wasm-libraries/user-host-trait/src/lib.rs12 C.WASMSecurityMeasuresforStylus13 hasheye 3OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

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

September6,2024Pre-projectkickoffcall September16,2024Deliveryofreportdraft September16,2024Reportreadoutmeeting September20,2024Deliveryofreportdraft October23,2024Deliveryoffinalsummaryreport hasheye 4OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

ProjectTargets Theengagementinvolvedareviewandtestingofthefollowingtargets. StylusEmergencyFixes Repository nitro-private (fixes) Version 0cc80646cff240d3f86cb8d6f6e8b9c83be9266b TypeGo,Rust PlatformArbitrum GovernanceArbOS32Actions Repository governance-private (PR#1) Version 2d42f247d0cc2ab4b8eb47f49dd2b322be9f9d1f TypeSolidity PlatformArbitrum hasheye 5OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

ExecutiveSummary EngagementOverview OffchainLabsengagedhasheyetoreviewthesecurityoffixesforanumberof high-severityissuesfoundafterStyluswasdeployed. AteamoftwoconsultantsconductedthereviewfromSeptember11toSeptember19, 2024,foratotaloftwoengineer-weeksofeffort.Withfullaccesstosourcecodeand documentation,weperformedamanualreviewoftheaffectedcodeandthefixes. ObservationsandImpact Duringtheengagement,weverifiedthattheproposedfixescompletelymitigatethe high-severityissuesfoundafterStyluswasdeployed,includinganactivationedgecasethat wasfoundduringthisengagement(TOB-STYLUS-FIX-1);notethatthisissuewasalsofound byOffchainLabsduringarefactoroftheaffectedcode. Additionally,wereviewedasetofgovernanceactionstoupgradeArbOStoversion32 (L1ModuleRootArbOneAction , L1ModuleRootNovaAction ,and L2ArbOS32Action)and twoemergencyactionsthatwillbeexecutedifStylusneedstobedisabled (SetInkPriceOneAction , SetWasmMaxStackDepthZeroAction). ThegovernanceactionswillupgradeArbOStoversion32andsetthenewmoduleroot hashonbothNovaandArbOne;additionally,theywillrevertanychangesmadebyeither oftheemergencyactions,effectivelyre-enablingStylusifeitheroftheemergencyactions wasexecuted;otherwise(i.e.,iftheemergencyactionswerenotexecuted),theywillsimply upgradetheArbOSversionandthemoduleroot. Alltheaforementionedactioncontractsarecorrect;additionally,weverifiedthatthe correctmodulerootha sh, 0x184884e1eb9fefdc158f6c8ac912bb183bf3cf83f0090317e0bc4ac5860baa39 ,is beingemployedinalltheactionsandconfirmedthatitistherootha shgeneratedbythe reviewedNitrochanges. Recommendations PerformanArbOSupgradewiththereviewedactions,eitherasanemergencyor nonemergencymeasure,dependingonwhethertheissuesareactivelyexploitableand whetheritislikelythattheissueswillbeidentifiedbythirdparties. hasheye 6OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

SummaryofFindings Thetablebelowsummarizesthefindingsofthereview,includingtypeandseveritydetails. IDTitleTypeSeverity 1Importingforward__set_trapproducesafailurein WASMinitialization Data Validation High hasheye 7OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

DetailedFindings 1.Importingforward__set_trapproducesafailureinWASMinstantiation Severity:HighDifficulty:Low Type:DataValidationFindingID:TOB-STYLUS-FIX-1 Target: forward_stub.wat Description UserscandeployaspeciallycraftedStylusprogramthatwillcauseArbOStopanicafterthe activationchecksarepassed. UserscanaccessavarietyofimportstocallintheirStylusprograms.Theseareincludedin the forward_stub.wat file: ;;allowsuser_hosttorequestatrap (global$trap(muti32)(i32.const0)) (func$checkunreachable) (func(export"forward__set_trap")unreachable) ;;userlinkage (func(export"vm_hooks__read_args") (parami32)unreachable) (func(export"vm_hooks__write_result")(parami32i32)unreachable) ... Figure1.1:Partofthe forward_stub.wat file Theimportsavailabletousersfromthe vm_hooks modulearepropertydocumentedand seemtoworkcorrectly,butthereisanadditionalimportavailablecalled forward__set_trap .UsingthisimportwillproduceavalidStylusprogramthatwill correctlypasstheactivationchecks. However,theimportsdefinedforWASMinstantiationareonlytheonesfromthe vm_hooks module. define_imports! ("vm_hooks"⇒host{ read_args,write_result,exit_early, storage_load_bytes32,storage_cache_bytes32,storage_flush_cache, transient_load_bytes32,transient_store_bytes32, call_contract,delegate_call_contract,static_call_contract,create1, create2,read_return_data,return_data_size, emit_log, hasheye 8OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

account_balance,account_code,account_codehash,account_code_size, evm_gas_left,evm_ink_left, block_basefee,chainid,block_coinbase,block_gas_limit,block_number, block_timestamp, contract_address, math_div,math_mod,math_pow,math_add_mod,math_mul_mod, msg_reentrant,msg_sender,msg_value, tx_gas_price,tx_ink_price,tx_origin, pay_for_memory_grow, native_keccak256, },); ... letinstance=Instance::new(&mutstore,&module,&imports)?;

Figure1.2:WASMinstantiationinArbOSusingtheWasmerAPI Tryingtoactivateastylusprogramthatimports forward__set_trap willproduceapanic intheArbOScode: thread'<unnamed>'panickedatstylus/src/util.rs:19:5: encounteredfatalwasm:initfailed Causedby: Errorwhileimporting"forward"."set_trap":unknownimport.Expected Function(FunctionType{params: [],results:[]}) Location: stylus/src/native.rs:207:24
Figure1.3:PartofthepanicerrorwhentryingtoactivateastylusprogramthatimportsforwardsetTrap
Notethatthisissuewasindependentlydiscoveredbytheoffchainlabsteamaswellasby hasheye,duringthisreview. ExploitScenario Evedeploysaspeciallycraftedstylusprogramthatimports forward__set_trap ,meaning thatitwillhaltthechainonceitisactivated. Recommendations Shortterm,removethe forward__set_trap exportfrom forward_stub.wat . Longterm,considercreatingacompletespecificationoftheallowedWASMproperties enforcedduringWASMactivationandincludeadditionaltestcases. hasheye 9OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

A.VulnerabilityCategories
Thefollowingtablesdescribethevulnerabilitycategories,severitylevels,anddifficulty levelsusedinthisdocument. VulnerabilityCategories CategoryDescription AccessControlsInsufficientauthorizationorassessmentofrights AuditingandLoggingInsufficientauditingofactionsorloggingofproblems AuthenticationImproperidentificationofusers ConfigurationMisconfiguredservers,devices,orsoftwarecomponents CryptographyAbreachofsystemconfidentialityorintegrity DataExposureExposureofsensitiveinformation DataValidationImproperrelianceonthestructureorvaluesofdata DenialofServiceAsystemfailurewithanavailabilityimpact ErrorReportingInsecureorinsufficientreportingoferrorconditions PatchingUseofanoutdatedsoftwarepackageorlibrary SessionManagementImproperidentificationofauthenticatedusers TestingInsufficienttestmethodologyortestcoverage TimingRaceconditionsorotherorder-of-operationsflaws UndefinedBehaviorUndefinedbehaviortriggeredwithinthesystem hasheye 10OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

SeverityLevels SeverityDescription InformationalTheissuedoesnotposeanimmediateriskbutisrelevanttosecuritybest practices. UndeterminedTheextentoftheriskwasnotdeterminedduringthisengagement. LowTheriskissmallorisnotonetheclienthasindicatedisimportant. MediumUserinformationisatrisk;exploitationcouldposereputational,legal,or moderatefinancialrisks. HighTheflawcouldaffectnumeroususersandhaveseriousreputational,legal, orfinancialimplications. DifficultyLevels DifficultyDescription UndeterminedThedifficultyofexploitationwasnotdeterminedduringthisengagement. LowTheflawiswellknown;publictoolsforitsexploitationexistorcanbe scripted. MediumAnattackermustwriteanexploitorwillneedin-depthknowledgeofthe system. HighAnattackermusthaveprivilegedaccesstothesystem,mayneedtoknow complextechnicaldetails,ormustdiscoverotherweaknessestoexploitthis issue. hasheye 11OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

B.CodeQualityRecommendations
Thefollowingrecommendationsarenotassociatedwithspecificvulnerabilities.However, theyenhancecodereadabilityandmaypreventtheintroductionofvulnerabilitiesinthe future. General • Considerusingthe must_use Rusthintinfunctionssuchas flush_storage_cache tomitigatethepossibilitythatthecallerwillignorethe returnvalue. arbitrator/wasm-libraries/user-host-trait/src/lib.rs • Considerexpandingthedocumentationofeachfunctioninthefiletoincludethe minimumandmaximumvalueofinkandgasthatneedstobechargedforevery call.Additionally,clearlynotewhetheraninternalfunctionhandlesthe computationalcostofeachoperation.Thiswillhelptopreventcomputationalcosts frombeingunderchargedorovercharged. • Relatedtothepreviousrecommendation,addunitteststocoveraverageand cornercasesintheink/gasusageforeachfunction. hasheye 12OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

C.WASMSecurityMeasuresforStylus
ThisappendixliststhecurrentsecuritymeasuresandconstraintscheckedduringWASM activation.ThesechecksguaranteethatWASMactivationproducesStylusprogramsthat aresecureandexecutecorrectly. Imports WASMimportshavethefollowingconstraints: • Ingeneral,onlythefunctionimportsavailableinthe forward_stub.wat fileare availabletouse. • Onlyfunctionimportsarevalid.WASMprogramsimportingotherentitiessuchas tablesormemorieswillimmediatelyfailvalidation. •

Theuseofimportswithvalidnamesbutincorrectsignatureswillimmediatelyfail validation. • Anyuseofimportswiththereservedprefix stylus_ willimmediatelyfailvalidation. However,wemustnotethefollowing: • Importscanbeduplicatedaslongastheyareconsistentandthenumberof duplicatesisnotdirectlylimited. • Importscanhavespecialcharacterssuchasthenullcharacter(\00). Exports Ingeneral,usersarefreetoexportanyfunctiontheyneed.However,therearenumberof constraints: • The user_entrypoint exportmustbeavailable,anditshouldhaveaspecific signature. • Exportnamescannotshadowanyimportnames,eithertherawname(e.g., pay_for_memory)orthefullcanonicalname(e.g., module__pay_for_memory). • Anyuseofexportswiththereservedprefix stylus_ willimmediatelyfailvalidation. • Somespecialglobalexportswillbeaddedtosupportinkmetering(e.g., stylus_ink_left).Theseexportsarecorrectlyaddedattheendoftheglobal indexspaceandcannotbeaccessedbyusersdirectly. • Exportscanhavespecialcharacterssuchasthenullcharacter(\00). hasheye 13OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment

AdditionalInternalFunctions
AnumberofinternalfunctionsareaddedintoWASMprogramsduringactivation.These functionsshouldneverbeuseddirectlybytheuser.Fortunately,callingthemisnot possiblesinceuserWASMprogramsarevalidatedtomakesurethefunctionindicesare correct,soaddingmoreinternalfunctionsissafeaslongastheyareaddedattheendof thefunctionindexspace. hasheye 14OffchainLabsStylusEmergencyFixes PUBLIC SecurityAssessment