HashEye

// SMART CONTRACT SECURITY AUDIT

Discord DAVE

Security assessment by HashEye · prepared for Discord

HASHEYE AUDITED

PROJECT	Discord DAVE
CLIENT	Discord
CATEGORY	Blockchain
PUBLISHED	August 1, 2024
REPORT ID	research-discord-dave-2024-08-01-15gs1z

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-discord-dave-2024-08-01-15gs1z.

DiscordDAVEProtocolDesign Review CryptographicDesignReview November16,2023 Preparedfor: MaximeNay Discord Preparedby:FredrikDahlgrenandTjadenHess

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 1DiscordDAVEProtocolCryptographicDesignReview PUBLIC

NoticesandRemarks CopyrightandDistribution Thisreportisconsideredbyhasheyetobepublicinformation;itislicensedtoDiscord underthetermsoftheprojectstatementofworkandhasbeenmadepublicatDiscord’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 2DiscordDAVEProtocolCryptographicDesignReview PUBLIC

TableofContents

B.GuidanceonUsingShortAES-GCMTags29 C.FixReviewResults30 DetailedFixReviewResults32 D.FixReviewStatusCategories34 hasheye 3DiscordDAVEProtocolCryptographicDesignReview PUBLIC

ProjectSummary ContactInformation Thefollowingprojectmanagerwasassociatedwiththisproject: AnneMarieBarry,ProjectManager annemarie.barry@hasheye.io Thefollowingengineeringdirectorwasassociatedwiththisproject: JimMiller,EngineeringDirector,Cryptography james.miller@hasheye.io Thefollowingconsultantswereassociatedwiththisproject: FredrikDahlgren,ConsultantTjadenHess,Consultant fredrik.dahlgren@hasheye.iotjaden.hess@hasheye.io ProjectTimeline Thesignificanteventsandmilestonesoftheprojectarelistedbelow. DateEvent September21,2023Pre-projectkickoffcall October2,2023Statusupdatemeeting#1 October10,2023Deliveryofreportdraft October10,2023Reportreadoutmeeting October17,2023Deliveryofcomprehensivereport hasheye 4DiscordDAVEProtocolCryptographicDesignReview PUBLIC

ExecutiveSummary EngagementOverview Discordengagedhasheyetoreviewthedesignofitsnewend-to-endencrypted(E2EE) RTCprotocolDAVE.Theprotocolaimstoprovideend-to-endencryptedvoiceandvideo callsforDiscordusers.ThedesignisbasedontheMLSauthenticatedkeyexchange mechanismandusesencryptedWebRTCforthemediatransport. Ateamoftwoconsultantsconductedthereviewfrom September25toOctober6,2023,for atotaloffourengineer-weeksofeffort.Ourtestingeffortsfocusedonensuringthatthe integrationwithMLSandthemediaencryptionspecifiedbytheDAVEprotocolsatisfiedthe protocol’ssecurityrequirements.Theworkwasperformedwithfullaccesstoprotocol designdocumentation,the mlspp librarysourcecode,andtheDiscordmonorepo. Additionally,weperformedafixreviewtoassesstheimplementedfixesfortheissues describedinthisreport.Outofthe11issuesidentifiedduringtheengagement,10issues werecompletelyaddressedbytheDiscordteam.Theresultsfromthefixrevieware describedinappendixC. ObservationsandImpact Atthetimeofthereview,theDiscordend-to-endencryptedRTCprotocolwasin developmentandnotfullyspecified.Findingsinthisreportrepresentplausiblesecurity issuesthatmayariseinafullyimplementedversionoftheprotocol,basedonthe documentationavailableatthetimeofthereview. Weidentifiedtwopotentialissuesrelatedtothevalidationof MLScredentialsandkey packagesinsidethe mlspp library(TOB-DISCE2EE-2andTOB-DISCE2EE-3).These validationsmustbeexplicitlyenforcedbytheDiscordE2EERTCprotocol. Ourreviewalsouncoveredtwoissuesrelatedtotheproposed MLSgroupevolution mechanisms,whichcouldpotentiallyallowmalicioususerstopreventtheadditionor removalofotherusers(TOB-DISCE2EE-1andTOB-DISCE2EE-5). Additionally,wefoundtwoissuesrelatedtotheproposeduserinterfaceandend-to-end verificationflowthatwouldmakeitharderforuserstodeterminewhethertheirsessions aresecureagainsteavesdroppers(TOB-DISCE2EE-6andTOB-DISCE2EE-7). Finally,wediscoveredtwoissuesrelatedtotheDAVEtransportencryptionscheme.We foundthattheinteractionbetweencodec-specificpacketizationandframeencryptionis complexandexposesalargeattacksurface(TOB-DISCE2EE-10andTOB-DISCE2EE-11).We recommendathoroughexaminationofthisinteractioninafutureimplementationreview. hasheye 5DiscordDAVEProtocolCryptographicDesignReview PUBLIC

Overall,wefoundtheprotocoltobewelldesigned,usingmodernprotocolsandprimitives forcontinuousgroupkeyagreementandtransportencryption.Carewastakentoidentify andmitigateanumberofdifferentthreatscenarios,andtheserisksandtheirmitigations arealsodescribedintheprotocoldesigndocument.Theweakestcomponentofthecurrent designisthespecificationofthecodec-awaremediaframeencryption,whereweseeareal riskofsensitivedatabeingleftunencryptedbyafutureimplementation. Recommendations Basedonthecodebasematurityevaluationandfindingsidentifiedduringthesecurity review,hasheyerecommendsthatDiscordtakethefollowingstepspriortodeploying theprotocolinaproductionenvironment: • Remediatethefindingsdisclosedinthisreport.Manyofthefindingsinthis reportconstituteasevererisktoeithertheconfidentiality,integrity,oravailabilityof userdata.Forthisreason,werecommendthatthesefindingsbeaddressedaspart ofadirectremediationbeforetheprotocolisdeployed. • DriveMLSgroupevolutionfromtheDiscordsignalingserver.Theproposed implementationreliesongroupmemberstoissueMLSproposalsandcommits.This allowsmultipledegreesoffreedomthatmalicioususerscanmisusetocause denial-of-serviceconditionsandotherunexpectedbehavior.ByrequiringallMLS proposalstobesubmittedbythecentralizedsignalingserverandbyvalidating commitsagainstagroupstatetrackedbytheserver,thisattacksurfacecanbe minimized. • Reviewandmonitorthecodec-dependentencryptionforcorrectness.The proposedimplementationofthecodec-dependentselectiveencryptionisbrittleand

pronetodisclosesensitivedatatoprivilegednetworknodes,suchastheselective forwardingunit(SFU).InitialfindingsindicatethatAV1-andH.264-encodedframes maydisclosesensitivemetadataabouttheencodedframeorevendisclosethe encodedframeitselfinsomecases. WerecommendthatDiscordreviewtheimplementationoftheWebRTCpacketizer anddepacketizertoensurethattheunencryptedportionsoftheframearerequired bytheWebRTCimplementationtodecomposeandthenreconstructtheframeand toensurethateverythingelseiseitherstrippedorencryptedbytheprotocol. WealsorecommendthattheDiscordteamsetupintegrationteststoensurethat emittedmediaframesconformtotheexpectedformatandthatsensitive informationaboutthemediastreamisnotleftunencryptedonanyofthe supportedplatforms. • Movetopacket-basedend-to-endencryptioniftherequisiteAPIsbecome available.TheRTPgenericheaderanddependencydescriptorextensionsare hasheye 6DiscordDAVEProtocolCryptographicDesignReview PUBLIC

currentlynotexposedbyWebRTCAPIsavailabletowebclients.Ifthesebecome availableinfutureversionsoftheAPI,itwouldbepossibletomovecodecheaders toanRTPheaderextensionandmakethetransportencryptorcodec-unawareby encryptingindividualRTPpacketsratherthanencodedframes.Thiswouldsimplify thetransportencryptionprotocolandmitigatetheriskofplaintextdisclosure.It wouldalsoavoidtherisksinvolvedwithrunningtheRTPdepacketizeron unauthenticatedinputdata.WerecommendthattheDiscordteammonitorthe WebRTCAPIssupportedbypopularbrowsersandupdatetheprotocolto packet-basedencryptionwhenthenecessaryAPIsbecomeavailable. • Performanin-depthcodereviewoncetheprotocolhasbeenimplemented. Thisengagementdidnotincludeafullreviewoftheimplementedprotocol.Afully implementedversionoftheend-to-endencryptionsystemwillcontain security-relevantedgecasesandnuancesnotcapturedbythehigh-levelprotocol description.Werecommendanespeciallythoroughreviewoftheprotocol's symmetricencryptionsystemandofMLScommitvalidations. FindingSeveritiesandCategories Thefollowingtablesprovidethenumberoffindingsbyseverityandcategory. EXPOSUREANALYSIS SeverityCount High4 Medium5 Low1 Informational1 Undetermined0 CATEGORYBREAKDOWN CategoryCount Authentication1 Cryptography4 DataValidation5 DenialofService1 hasheye 7DiscordDAVEProtocolCryptographicDesignReview PUBLIC

ProjectGoals Theengagementwasscopedtoprovideadesignreviewoftheprotocol. Specifically,wesoughttoanswerthefollowingnon-exhaustivelistofquestions: • HowaretheMLSauthenticationanddeliveryservicesimplemented,andwhat securitypropertiesdotheyprovide? • WhichtypesofMLSproposalsareallowed,andhowaretheyvalidated? • Areaccesscontrolsinplacetopreventusersfromaddingorremovingother membersfromanexistinggroup? • WhichgroupmembersmayissueanMLScommit? • HowareinvalidMLScommitshandled,andhowarevalidMLScommitsagreed upon? • Doestheprotocolprotectagainstspam? • Whichtypesofidentitiesaresupportedbytheprotocol? • Howareidentitiesauthenticatedbyandbypeers? • Howarecredentialrevocationandexpirationhandledbytheprotocol? • Howispost-compromisesecurityguaranteedbytheprotocol? • Aretransportencryptionkeysupdatedwitheachnewepoch? • Aretransportencryptionkeysderivedsecurely? • Doesthesystemproperlyprotectagainst-GCMkeywear-out? • Howareunencryptedandmediacodecheadersauthenticated? • Howismisusereportingimplemented? • Howdoesthekeyagreementprotocolresistmachine-in-the-middleand impersonationattacks? hasheye 8DiscordDAVEProtocolCryptographicDesignReview PUBLIC

ProjectTargets Theengagementinvolvedareviewofthetargetslistedbelow. RTCE2Eprotocol VersionSeptember21,2023 TypeDesigndocument Discordmonorepo Repositoryhttps://github.com/discord/discord Version a02db9bc34e6bbc5b1eb1e0149d7b056828afacc TypeC++ PlatformMultiple mlspp Repositoryhttps://github.com/cisco/mlspp Version 8a010ef9ce9f1bdd8b79a11ee1c089440a3f63fb TypeC++ PlatformMultiple hasheye 9DiscordDAVEProtocolCryptographicDesignReview PUBLIC

ProjectCoverage Thissectionprovidesanoverviewoftheanalysiscoverageofthereview,asdeterminedby ourhigh-levelengagementgoals.Ourapproachesincludedthefollowing: • MLS-basedcontinuouskeyagreement.Weperformedanin-depthreviewofthe MLS-basedkeyagreementprotocoldefinedbythedesigndocument.Thisreview wasbasedbothonthedesigndocumentitselfandonexternalreferenceslikethe MLSRFCandtheMLSarchitecturedocument.WefocusedonhowMLSmessages arevalidatedbygroupmembersandbythedeliveryservice(DS)andhowidentities andcredentialsaremanagedbytheauthenticationservice(AS).Wealso investigatedwaysforindividualmemberstopreventtheprotocolfrommaking progress. • DAVEtransportencryption.WereviewedthedesignoftheDAVEprotocol's media

encryption,payingspecialattentiontotheselectiveencryptionofencodedmedia frames.Thispartoftheengagemententailedanextensivereviewofexternal documentationforthedifferentcodecsinvolvedtounderstandwhetherthe proposeddesigncouldeitherdisclosesensitivedataaboutthemediastreamorbe vulnerabletotamperingorimpersonationattacks. CoverageLimitations Becauseofthetime-boxednatureoftestingwork,itiscommontoencountercoverage limitations.Thefollowinglistoutlinesthecoveragelimitationsoftheengagementand indicatessystemelementsthatmaywarrantfurtherreview: • WewereunabletoobtainconclusiveresultsontheexactH.264networkabstraction layers(NALs)andAV1openbitstreamunits(OBUs)thatmustbeencryptedtofully protecttheconfidentialityofthemediastream.Thatsaid,initialresultsindicatethat thecurrentdesignmayleavesomemediaframesunencrypted(TOB-DISCE2EE-10). • Weusedtheprovidedcodebaseasareferencetobetterunderstandthespecificationbutdidnotperformanin-depthreviewoftheimplementedcodeitself. hasheye 10DiscordDAVEProtocolCryptographicDesignReview PUBLIC

SummaryofFindings Thetablebelowsummarizesthefindingsofthereview,includingtypeandseveritydetails. IDTitleTypeSeverity 1CommitspamcouldpreventgroupupdatesDenialofServiceMedium 2Commitleafnodesarenotvalidatedbythemlspp library DataValidationMedium 3Themlspplibrarydoesnotvalidatekeypackage lifetimes DataValidationInformational 4Webclientmayallowamaliciousserverto conductamachine-in-the-middleattackonthe session CryptographyHigh 5CommittingmembersmayfailtosendWelcome messages DataValidationMedium 6Userscoulddecryptmessagesafterbeing removedfromthecallUI DataValidationHigh 7Keyfingerprintverificationisvulnerabletopartial preimageattacks AuthenticationMedium 8Abusereportingmechanismisvulnerableto messageforgery DataValidationMedium 9DAVE’smediaencryptionprovidesweakened forwardsecrecyguarantees CryptographyLow 10TheprotocolmayfailtoencryptAV1-encoded mediaframes CryptographyHigh 11Videoframeheaderlengthandheaderdataare notauthenticated CryptographyHigh hasheye 11DiscordDAVEProtocolCryptographicDesignReview PUBLIC

DetailedFindings 1.Commitspamcouldpreventgroupupdates Severity:MediumDifficulty:Undetermined Type:DenialofServiceFindingID:TOB-DISCE2EE-1 Target:E2EERTCprotocol Description Thesectiononcommitorderinginthedesigndocumentstatesthatthesignalingserverwill broadcastthefirstcommitseenforeachepochtoallmembersofthegroup.Ifa committingmemberstartsspammingthegroupwithnewcommits,thiscouldeffectively preventothermembersfromcommitting,whichwouldpreventmeaningfulgroupupdates andcauseunnecessaryloadonthesymmetricencryptionmechanism. Thesectiononkeyrotationmentionsratelimitingemptycommitstoavoidunnecessary keyupdates.Thismayalsomitigatethisissue,dependingonhowthesystemhandles Add and Remove proposals.Thedocumentationstatesthefollowingrestrictionson Add and Remove proposals: Commitsincludingaddproposalsareonlyvalidiftheaddedmemberispresentinthe memberlistreceivedfromthedeliveryservice. Commitsincludingremovalproposalsareonlyvalidiftheremovedmemberisremoved fromthememberlistreceivedfromthedeliveryservice. However,ifamembercaninclude Add and Remove proposalsformemberswhowere previouslyaddedorremovedfromthegroup,thiscouldstillbeanissue. ExploitScenario Amalicioususerwithaprivilegednetworkpositionspamsthenetworkwithcommits containing Add and Remove proposalsforpreviousmembers(whohavealreadybeen addedandremovedoncefromthegroup).Sincetheserverbroadcastsonlythefirst commitobtainedineachepoch,thiseffectivelypreventsanyoneelsefromcommittingto thegroup.Inparticular,newmemberscannotbeadded,andthemalicioususercannotbe removed. hasheye 12DiscordDAVEProtocolCryptographicDesignReview PUBLIC

Recommendations Shortterm,disallowemptycommitstothegroupwhentherearеoutstanding Add or Remove proposalstothegroup. Longterm,disallowgroupmembersfromsubmittinganyproposalsandinsteaduse externalproposalstoaddandremovemembers.RequiretheDStobroadcastonly commitsthatcontainthefullsetofcurrentproposals,andvalidatethecommitstoensure thatallcredentialsareauthentic.Keyrotationmaybeimplementedbyexternal Psk proposals.FortheDStovalidatehandshakemessages,theymustbesentasunencrypted PublicMessage objects.Thesehandshakemessagesshouldbepoint-to-pointencrypted andauthenticatedusingTLS. hasheye 13DiscordDAVEProtocolCryptographicDesignReview PUBLIC

2.Commitleafnodesarenotvalidatedbythemlspplibrary Severity:MediumDifficulty:Medium Type:DataValidationFindingID:TOB-DISCE2EE-2 Target: src/state.cpp in mlspp Description AcommittingmembercanupdatetheirownleafnodewithanemptycommitThenewleaf nodeisvalidatedbythe mlspp library,butthelibrarydoesnotcheckthatthecredential andsigningkeyinthenewleafnodematchthoseinthereplacednode.Thismeansthat

memberscanupdatetheiridentitiesintheratchettree. bool State::valid(constLeafNode&leaf_node, LeafNodeSourcerequired_source, std::optional<LeafIndex>index)const { //VerifythatthecredentialintheLeafNodeisvalidasdescribedinSection //5.3.1. //XXX(RLB)N/A,nocredentialvalidationinthelibraryrightnow // ... return(signature_valid&&supports_group_extensions&&correct_source&& mutual_credential_support&&supports_own_extensions); } Figure2.1:Credentialsarenotvalidatedbythe mlspp library. (mlspp/src/state.cpp#L1442-L1503) Iftheratchettreeisincludedwiththe Welcome messagetonewmembers,theupdated identitywillbepropagatedtofuturemembersjoiningthegroup. ExploitScenario Amalicioususerregisterspersistentkeysfortwodifferentidentities,S 1 andS 2 ,with Discord.DuringasessionwheretheuserisacommittingmemberasS 1 ,theysenda commitreplacingtheirleafnodewithanewnodecontainingS 2 ,alongwiththe correspondingsigningkey.Thisintroducesariskthatjoiningmemberswillmisidentifythe malicioususerasS 2 ,whereaspreviousmembersinthegroupstillseetheuserasS 1 . Recommendations Shortterm,validatecommitmessagestoensurethatexistinggroupmembercredentials arenotreplacedbyacommit. hasheye 14DiscordDAVEProtocolCryptographicDesignReview PUBLIC

Longterm,considerperforminganinternalsecurityreviewofthe mlspp librarytobetter understandthematurityofthecodebase. hasheye 15DiscordDAVEProtocolCryptographicDesignReview PUBLIC

3.Themlspplibrarydoesnotvalidatekeypackagelifetimes Severity:InformationalDifficulty:NotApplicable Type:DataValidationFindingID:TOB-DISCE2EE-3 Target:E2EERTCprotocol Description MLSkeypackagescontaina lifetime fieldthatdeterminesthevalidityperiodofthekey package.The mlspp librarydoesnotvalidatethesevalues. //TODO(RLB)Verifythelifetimefield Figure3.1:Missingkeypackagelifetimevalidation(mlspp/src/state.cpp#1475-1477) Thecurrentprotocoldoesnotcachekeypackagesbeyondasinglesession,sothelifetime fieldmaybesettothemaximumvalue.However,iffutureversionsoftheprotocoluse cachedkeypackages,itwillbeimportanttoaddlifetimevalidationontopofthevalidations that mlspp performs. Recommendations Shortterm,setthekeypackagelifetime not_before and not_after parameterstothe maximumallowedtimespantoavoidkeypackagesexpiring. Longterm,verifywhichvalidationsspecifiedbyRFC9420areincludedin mlspp andadd anymissingcheckstotheDiscordcodebase. hasheye 16DiscordDAVEProtocolCryptographicDesignReview PUBLIC

4.Webclientmayallowamaliciousservertoconducta machine-in-the-middleattackonthesession Severity:HighDifficulty:High Type:CryptographyFindingID:TOB-DISCE2EE-4 Target:E2EERTCprotocol Description TheDiscordwebclientstoreskeymaterialinthebrowser,makingitaccessibletoany JavaScriptcodeservedbyDiscordoranadversarywithaccesstoaTLScertificatefor discord.com . Unlikemobileordesktopclients,thewebclientcodeisservedtotheuthereverytimethey opentheapp.Thedeliveredcodemaydifferdependingontheuserrequestingit,anditis notsignedwithacodesigningkey,unlikemobileappsdeliveredbyappstores.Webapp usersarethusatincreasedriskofimpersonationandmachine-in-the-middleattacksdueto malicioucode. ExploitScenario Anation-stateattackerownsaTLSrootcertificateandissuesafraudulentcertificatefor discord.com .Theattackerinterceptstrafficfromspecificusersandreplacestheirdiscord applicationwithabackdooredversion.Theattackercantheneavesdroponandtamper withallfurthercommunicationbytheusers. Recommendations Shortterm,warnusersthatthesecurityguaranteesofferedbythewebclientareweaker thanthoseofferedbythemobileordesktopapplications. Longterm,considerimplementingabrowserextensiontoenablecodesignature verificationandcodefingerprintverification.Foranexampleofhowthiscouldbedone,see thisblogpostonMeta’sCodeVerifybrowserplugin. hasheye 17DiscordDAVEProtocolCryptographicDesignReview PUBLIC

5.CommittingmembersmayfailtosendWelcomemessages Severity:MediumDifficulty:High Type:DataValidationFindingID:TOB-DISCE2EE-5 Target:E2EERTCprotocol Description ToinviteanewmembertoanMLSgroup,acommittingmembermustsenda commit containingan Add proposal.Assumingtheprotocolusespublichandshakemessages,a signalingservercanensurethatthistakesplacecorrectly.However,afterallusersprocess thecommit,thecommittingmembermustsenda Welcome messagetothejoinersothe joinercaninitializetheirratchettreestateandbegindecryptingmessages.This Welcome messageisencrypted,sothesignalingservercannotdeterminewhetheritiscorrectly formed. OnepossiblesolutiontothisissueistorequireeachjoinertoconfirmtotheDSthatthey havereceivedavalid Welcome message.Aftersometimeout,theDScouldthenorchestrate aretryoftheaddition.However,thejoinermaylieaboutreceivinganinvalid Welcome message,andwhenmultiplejoinersareaddedinasingleepoch,theymaydisagreeasto thevalidityofthe Welcome message.Thisaddscomplexitytothenewmemberaddition processandmakesadenialofservicemorelikely. ExploitScenario Amalicioususerwantstopreventnewmembersfrombeingaddedtoagroup.Whenthe DSannouncesanewmember,theusercommitsthe Add proposal,butneversendsa Welcome

message.Thejoininguseristhenunabletodecryptmessagesandenterthecall. Recommendations Shortterm,havethesignalingservermonitorcommitsaddingnewmemberstoensurethe committersendsacorresponding Welcome message.Ifno Welcome issent,theserver shouldremovethecommitterfromthegroupofcommittingmembersandrequestanew Welcome messagefromthegroup.Ifthenewmemberrejectsthe Welcome messageas invalid,theservershouldsimplyrequestanew Welcome fromarandomcommitting memberofthegroup. Longterm,considerusingthe ExternalInit flowtoaddnewmemberstoagroup.The DSservesacachedcopyofthecurrent GroupInfo structtothenewmember,whothen submitsanexternalcommittothegroup,addingthemselves.Thisremovestheneedfor anyexistinggroupmembertocoordinatetheadditionofnewmembers. hasheye 18DiscordDAVEProtocolCryptographicDesignReview PUBLIC

6.Userscoulddecryptmessagesafterbeingremovedfromthecall UI Severity:HighDifficulty:High Type:DataValidationFindingID:TOB-DISCE2EE-6 Target:E2EERTCprotocol Description TheclientUIlistingtheusersthatareconnectedtoagivensessioniscontrolledbythe voicestateofthecorrespondingusers.Thisstateisnotdirectlycontrolledby Add or Remove messagesfromthesignalingserverorthecorrespondinggroupepochupdates.In practice,thismeansthatausermayberemovedfromtheUIbeforethegroupepochis updated,allowingtheusertocontinuetodecryptmessagestothesession,eventhough theyappeardisconnectedfromthepointofviewofothermembers. SuchauserwouldneedtointerceptWebRTCmessagesbetweenotherusersafterbeing removedfromtheSFU,whichwouldbefeasibleasapassivenetworkadversary. Additionally,anactivenetworkadversarymaybeabletoimpersonatecurrentgroup membersusingtheirknowledgeofothermembers’senderkeys. ExploitScenario Mallory,amaliciousnetworkadversaryconvincesamemberofavoicegrouptoaddherto thegroupbyimpersonatingadesiredgroupmember.UponrealizingthatMalloryisnotthe intendedgroupmember,theexistingmemberskickherfromthegroup.Malloryis removedfromtheDiscordUIandthegroupmemberscontinuediscussingsensitive information.Bydelayinghandshakemessages,MallorykeepstheMLSepochfrom advancinganduseshernetworkpositiontointerceptanddecryptencryptedframes,thus spyingundetectedontheconversation. Recommendations Shortterm,ensurethatusersarenotdroppedfromthelistofparticipantsuntilthe symmetrickeysusedtoencryptapplicationdataareupdated.Untilthegroupepochis updatedandanewsymmetrickeyisderived,theUImaydisplayusersasgrayedout. Longterm,ensurethattheMLSratchettreestateandidentitiesareauditablebytheend userandthattheUIclearlyreflectswhatidentitiescandecryptpacketsfromagivenE2EE session. hasheye 19DiscordDAVEProtocolCryptographicDesignReview PUBLIC

7.Keyfingerprintverificationisvulnerabletopartialpreimageattacks Severity:MediumDifficulty:High Type:AuthenticationFindingID:TOB-DISCE2EE-7 Target:E2EERTCprotocol Description TheDiscordclientwillallowuserstoverifythesigningkeysassociatedwithaparticular devicepair.Thisisdonebycomputingtworepeated SHA-512hashesovertheuser’s identityandthepublickeyassociatedwiththedevice,resultingina64-bytefingerprintthat consistsoftwoconcatenated SHA-512digests.Thesefingerprintsmaythenbeverifiedout ofband(e.g.,bymeetingandcomparingfingerprints). However,itiswellknownthatmanualverificationoflonghexadecimalvaluesiserror-prone.Thiscouldallowanattackertoimpersonateotherusersbycreatingakeypairwitha fingerprintthatissimilarenoughtotheimpersonateduser.(TheDEAwassubjecttoan attackofthistypeearlierthisyear,whichledtothelossof50,000USD.) ExploitScenario Anation-stateattackerwhocanconductamachine-in-the-middleattackonAlice’s connectiongeneratesasigningkeywhosefingerprinthasthesamefirstfourbytesandlast fourbytesasAlice’sfingerprint.Theattackerregisterstheirkeyfor Alice’saccountand impersonatesAliceincalls.WhenAliceandBobmeettoverifytheirsigningkeyfingerprints outofband,Bobcomputeshisfingerprintusingtheattacker's key.AliceandBobfailto noticethisbecausetheyonlycomparethefirstandlastdigitsofthefingerprint. Recommendations Shortterm,encodethefingerprintasaQRcodetoallowuserstoverifyitautomaticallyif theirdevicehasacamerathatcanscanQRcodes.Usethemanualverificationprocessasa fallbackonly,anddirectuserstousetheQRcodewheneverpossible. Longterm,reviewuserstudiesonfingerprintverificationandchooseaformat(e.g., sentence-basedfingerprints)thatislesssusceptibletopartialpreimageattacks. hasheye 20DiscordDAVEProtocolCryptographicDesignReview PUBLIC

8.Abusereportingmechanismisvulnerabletomessageforgery Severity:MediumDifficulty:High Type:DataValidationFindingID:TOB-DISCE2EE-8 Target:E2EERTCprotocol Description Thecurrentiterationoftheprotocoldoesnotcontainamechanismforreportingabusive content.However,theDiscordteamisplanningtoimplementthisinafutureversionofthe

protocolbyallowinguserstocapturevoiceandvideostreamsandsubmitthesetothe DiscordTrustandSafetyteamtoreview.Sincethereisnowaytoauthenticatethecaptured streams,thismechanismisvulnerabletoforgeryattackswherethereportercreatesafake mediastreamandsubmitsthisasareportagainstanotherDiscorduser. ExploitScenario AliceusesanonlineAIvoiceandvideogeneratortocreateafakerecordingofavideocall withBob.ShesubmitsthistoDiscordasproofofabusivebehavior,andasaresult,Bobis bannedfromtheplatform. Recommendations Shortterm,investigatesolutionsbasedonmessagefranking(seetheAbuseReporting sectioninthiswhitepaperonFacebookMessenger),wherethesendercomputesabinding commitmenttotheplaintextframes,whichiseithersymmetricallyorasymmetrically authenticatedbytheserver.Thisoffloadsanystoragerequirementstothereceivingclient, whoneedstostoremediaandfrankingtagsonlyifanabusereportisactivelybeing recorded.Toreducethebandwidthrequirementsofthesystem,frankingtagsmaybe computedoveranumberofplaintextframes. Longterm,revisittheliteratureonmessagefrankinginthefuturetoseeifnewandmore lightweightschemesareproposedfortheWebRTCsetting. hasheye 21DiscordDAVEProtocolCryptographicDesignReview PUBLIC

9.DAVE’smediaencryptionprovidesweakenedforwardsecrecyguarantees Severity:LowDifficulty:High Type:CryptographyFindingID:TOB-DISCE2EE-9 Target:E2EERTCprotocol Description TheDAVEprotocolupdatesthesymmetricencryptionkeywheneverMLStransitionstoa newepoch.Thisprovidesforwardsecrecyandpost-compromisesecuritybetweendifferent MLSepochs.TheMLSprotocolalsoincludesasymmetricratchetmechanismcalleda secrettree,whichcanbeusedtoregularlyupdatesymmetrickeyswithinagivenepoch. ThissymmetricratchetalsoprovidesforwardsecrecyguaranteeswithinasingleepochThe currentprotocoldesigndoesnotusetheMLSsymmetricratchet,whichmeansthatthe forwardsecrecyguaranteesprovidedbythedesignareweakerthantheyshouldbe.Thisis particularlytrueforlong-livedepochswherenousersjoinorleavethesession. ExploitScenario Eve,anattacker,canstoreencryptedframesfromAlice,whoisparticipatinginagroupcall. Atsomepoint,EvecompromisesAlice'ssymmetrickey.Sincetheprotocoldoesnotratchet symmetrickeys,EvecangobackanddecryptallofAlice’smessagessentduringthecurrent epoch. Recommendations Shortterm,usetheMLSsecrettreetoderivesymmetricencryptionkeysandnonces.The mlspp librarydoesnotexposethesecrettreedirectly,butitispossibletoinstantiateanew secrettree(asan mlsppGroupKeySource struct)basedonthe exporter_secret key. Thesecureframenoncecanberepurposedastwo16-bitepochandgenerationcounters toensurethatthesendingandreceivingpartiesbothagreeonthecurrentepochand ratchetgeneration. hasheye 22DiscordDAVEProtocolCryptographicDesignReview PUBLIC

10.TheprotocolmayfailtoencryptAV1-encodedmediaframes Severity:HighDifficulty:High Type:CryptographyFindingID:TOB-DISCE2EE-10 Target:E2EERTCprotocol Description InthecurrentdesignoftheDAVEprotocol,AV1-encodedframesareonlypartially encrypted.Moreprecisely,theencryptorassumesthateachframecontainsatmostone frameOBUandthatthisisthelastOBUintheframe.TheframeOBUpayloadisthen encrypted,leavingtheOBUheaderandtheremainingOBUsunencrypted. However,accordingtosection6.9oftheAV1specification,aframeOBUissimplyamore compactrepresentationofaframeheaderOBU,followedbyatilegroupOBU,andthe sameframecould,inprinciple,berepresentedeitherway: AframeOBUconsistsofaframeheaderOBUandatilegroupOBUpackedintoasingle OBU. Theintentionistoprovideamorecompactwayofcodingthecommonusecasewhere theframeheaderisimmediatelyfollowedbytilegroupdata. IftheAV1encoderusesseparateframeheaderandtilegroupOBUstorepresentthe frame,theOBUswouldnotbeencryptedbythesenderunderthecurrentdesign.This wouldimmediatelydisclosethecurrentframeofthesender'smediastreamtotheSFU. ThesectiononorderingOBUs(section7.5intheAV1specification)seemstorequirethat frameOBUsandtilegroupOBUsbeplacedlastintheencodedframe,butthesectionalso mentionsthat“Someapplicationsmaychoosetousebitstreamsthatarenotfullyconformant totherequirementsdescribedinthissection.”Inpractice,thismeansthatnonconformant encodersmaydiscloseframeandtilegroupOBUs. ExploitScenario Alice’sDiscordclientusesAV1toencodehermediastream.Thestreamisencodedusing separateframeheaderandtilegroupOBUs,causingAlice’sclienttosendtheentiremedia streaminplaintexttotheserver,thusbreakingtheprotocol’send-to-endconfidentiality guarantees. hasheye 23DiscordDAVEProtocolCryptographicDesignReview PUBLIC

Recommendations Shortterm,testwhichtypesofOBUsareemittedbythedifferentDiscordclient implementationstoensurethatthemediastreamisencryptedcorrectlybyeachclient.At leastthefollowingOBUsshouldbeencryptedtopreservethemediastream’s confidentiality: • FrameheaderOBUs:Containmetadatadescribinghowthecurrentframehas changedcomparedtopreviousframes •

TilegroupUBUs:Containtiledataassociatedwiththeframe • TilelistOBUs:Containtiledatasimilartoatilegroup OBU,togetherwithadditional headersallowingthedecodertoprocesspartsofthecurrentframe (TilelistOBUsarecurrentlydroppedbytheWebRTCpacketizeraccordingtothe documentationprovidedbyDiscord.) Longterm,encryptframeheader,tilegroup,andframeOBUsindependentoftheir positionintheencodedframe.ReviewtheAV1specificationindetailtoensurethatuser dataisnotdisclosedbytheremainingOBUs. References • ATechnicalOverviewofAV1 • AV1Bitstream&DecodingProcessSpecification

11.Videoframeheaderlengthandheaderdataarenotauthenticated Severity:HighDifficulty:High Type:CryptographyFindingID:TOB-DISCE2EE-11 Target:E2EERTCprotocol Description Becausepacketizationanddepacketizationrelyonvalueslocatedintheframepayload,a contiguousinitialportionofeachframeisleftunencrypted.Currently,thedesigndoesnot includetheseunencryptedheadersintheassociateddataofAES-GCM.AmaliciousSFU couldthusmodifytheseheadersundetected. OfparticularconcernaretheH.264/H.265andAV1frames,whichcontainvariable-length unencryptedheaderdata.Becausetheunencryptedheaderframesizevalueisnot authenticated,amaliciousSFUcanreplaceitwithalargervalue.TheSFUcantheninclude additionalunencryptedvideo-codinglayers,whichwillbecopieddirectlyintotheoutput frame.Additionally,ifnoncereplayprotectionsarenotpresentonthedecryptorside,the SFUcouldusethenonceandauthenticationtagfromafullyunencryptedheader-only frametoforgearbitraryplaintextframes. 66if(codecUnencryptedHeaderBytes){ 67//copytheunencryptedheadertotheoutputframe 68memcpy(frame.data(),encryptedFrame.data(),codecUnencryptedHeaderBytes); 69} Figure11.1:Unauthenticateddataisdirectlyincludedinthevisibleframe. (discord/discord_common/native/secure_frames/decryptor.cpp#66–69) AllowingtheSFUtoincludeorreplacecontentinusermediaframeswouldallow impersonationofusersbytheDiscordserver,evenwhenMLSend-to-endpersistent identityverificationisinuse.Additionally,unauthenticatedcodecheaderspresentalarge surfaceareaforexploitationofimplementationflawsintheunderlyingcodecs. Furthermore,lackofheaderauthenticationmayopenclientstoadaptiveattacksagainst confidentiality.Forexample,forgedvideo-codinglayersmayreferenceelementsdefinedin encryptedvideo-codinglayers,disclosinginformationabouttheencryptedlayersby observingdifferentialfailuresinthedecoder. ExploitScenario AmaliciousDiscordemployeemodifiestheSFUtoaddvideocodecNALsthatreplacea particularuser’sbroadcaststreamwithapre-recordedvideofakedtolooklikealegitimate

stream.Advanceduserschecktheperistentidentityfingerprintandareconvincedthatthe streamislegitimate. Recommendations Shortterm,includeallunencryptedcomponentsofmediaframesintheauthenticateddata oftheunderlyingAEAD. Longterm,keepabreastofnewextensionstotheWebRTCAPIsthatwouldallowDiscordto switchtoapacket-basedtransportencryptionmechanism.Thiswouldallowafuture versionoftheprotocoltoencryptmediacontentandheadersattheRTPpacketlevel, whichwouldallowtheprotocoltoencryptandauthenticatetheentireencodedframeina waythatwouldbeinvisibletotheRTPpacketizeranddepacketizer.

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

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
28DiscordDAVEProtocolCryptographicDesignReview PUBLIC

B.GuidanceonUsingShortAES-GCMTags
ThisappendixlistsconsiderationsthatmustbeobservedwhenusingtruncatedAES-GCM tags.WhileNISTSP800-38Dpermitstheuseof32-and64-bitauthenticationtagsinsome real-timeapplications,certainpropertiesofAES-GCMmakeshorttagsdangerousinmany situations.
WerecommendGCMtaglengthsof64bitsataminimumandatleast96bitsifpossible.
OtherAEADsbasedonHMACsratherthanpolynomialMACsaremorerobusttousewith truncatedtags.
TwopropertiesofAES-GCM,detailedinAuthenticationweaknessesinGCM,impactthe securityofschemesusingtruncatedGCMtags:
1.Longmessagesdecreasetheeffortrequiredtoconstructaforgery.Ifan adversaryobservesaproperlyauthenticatedmessageofbitlength2 k ,withtag length t ,thentheadversarycanforgeadifferentmessagewithaprobabilityof roughly2 (t-k) .Asaconcreteexample,ifanhonestusersendsa128-KBpacketusing a32-bittag,thentheadversarywillneedtosendroughly2 22 messagesbefore findingasuccessfulforgery.
2.Forgeriesagainsttruncatedtagsdiscloseinformationaboutthe authenticationkey.Ifanadversarycandeterminewhichforgeryattemptsare successful,theycanusethatinformationtoincreasetheprobabilityoffuture forgeries,eventuallyrevealingthefullauthenticationkey. NISTSP800-38D:AppendixCspecifiesrequirementsandguidelinesforusingshorttags; wesummarizethoserelevanttotheDiscordDAVEprotocol:
1.Donotrevealinformationaboutdecryptionsuccessforindividualpackets.In particular,donotsendretryrequestsforframesthatfailauthentication.Consider mitigatingtimingsidechannelssothatexternallyvisibletimingbehaviorissimilar fordecryptionsuccessorfailure.
2.Includeaslittleencrypted/authenticateddataaspossibleineachframe.Beawareof opportunitiesforadversaries,suchastheSFU,torequesttheencryptionor authenticationoflargeframes.
3.Designthesystemtoberobustagainstindividualframeforgeries.Forgeryofa singleframeshouldresultinonlyaminorchangeintheenduser’smediastream andshouldnotcausesystem-wideeffects. 4.Rotatesenderkeysfrequently,preferablyviasymmetricderivation.Asymmetrickey rotationviaMLScommitsmaybeselectivelydelayedbyamaliciousDS. hasheye
29DiscordDAVEProtocolCryptographicDesignReview PUBLIC

C.FixReviewResults Whenundertakingafixreview,hasheyereviewsthefixesimplementedforissues identifiedintheoriginalreport.Thisworkinvolvesareviewofspecificareasoftheupdated protocoldesigndocumentation,notcomprehensiveanalysisoftheentiresystem.
OnNovember9,2023,hasheyereviewedthefixesandmitigationsimplementedbythe Discordteamfortheissuesidentifiedinthisreport.Wereviewedeachfixtodetermineits effectivenessinresolvingtheassociatedissue.
Insummary,ofthe11issuesdescribedinthisreport,Discordhasresolved10issuesand haspartiallyresolvedtheoneremainingissue.Foradditionalinformation,pleaseseethe DetailedFixReviewResultsbelow. IDTitleStatus 1CommitspamcouldpreventgroupupdatesResolved
2CommitleafnodesarenotvalidatedbythemlspplibraryResolved
3ThemlspplibrarydoesnotvalidatekeypackagelifetimesResolved
4Webclientmayallowamaliciousservertoconducta machine-in-the-middleattackonthesession Resolved
5CommittingmembersmayfailtosendWelcomemessagesResolved
6UserscoulddecryptmessagesafterbeingremovedfromthecallUIResolved
7KeyfingerprintverificationisvulnerabletopartialpreimageattacksResolved
8AbusereportingmechanismisvulnerabletomessageforgeryPartially Resolved
9Secureframesencryptionprovidesweakenedforwardsecrecy guarantees Resolved hasheye
30DiscordDAVEProtocolCryptographicDesignReview PUBLIC

10SecureframesmayfailtoencryptAV1-encodedmediaframesResolved
11VideoframeheaderlengthandheaderdataarenotauthenticatedResolved hasheye

DetailedFixReviewResults TOB-DISCE2EE-1:Commitspamcouldpreventgroupupdates
Resolved.TheDShasbeenaddedasanexternalsenderandistheonlyoneallowedto
makeproposalstothegroup.Commitmessagesarefilteredbythe DS,whichacceptsonly
commitscontainingallthecurrentlyopenAddandRemoveproposalsmadebytheDS. TOB-DISCE2EE-
2:Commitleafnodesarenotvalidatedbythemlspplibrary
Resolved.BoththeDSandtheindividualmembersofthegroupnowvalidateallcommits
toensurethatmembercredentialsandsigningkeysarenotupdatedbythecommit.
TheDiscordteamhasalsodecidedtoperformaninternalreviewofthe mlspp libraryto
identifyanypotentialsecurityissuesinit.Anyissuesidentifiedwillbeaddressedandthefix
willbemergedupstreamto mlspp . TOB-DISCE2EE-3:Themlspplibrarydoesnotvalidatekeypackagelifetimes
Resolved.TheDSnowensuresthatthekeypackagefields not_before and not_after are
settothemaximumallowedlifespan. TOB-DISCE2EE-4:Webclientmayallowamaliciousservertoconducta machine-
in-the-middleattackonthesession
Resolved.TheDiscordteamwillinformusersthattheDiscordwebclientcannotofferthe
samesecurityguaranteesasnativeclientsagainstmachine-in-the-middleattacks. TOB-DISCE2EE-
5:CommittingmembersmayfailtosendWelcomemessages
Resolved.TheDSnowrequiresthecommittingmembertoincludethe Welcome message withthecorresponding
Commit .Ifamemberfailstotransmit Welcome messages,theymay
beremovedfromthegroupofcommittingmembers.Ifa Welcome messageisreportedas
invalidbythejoiningmember,theDSmayrequestanew Welcome messagefroma differentmemberofthegroup. TOB-
DISCE2EE-6:Userscoulddecryptmessagesafterbeingremovedfromthecall UI
Resolved.OfficialDiscordclientswillbeabletoreviewthecurrentMLSgroupstatetoseeif
leavingmemberscanstilldecryptmessagestothegroup.AccordingtothesectiononUI
considerations,thisshouldalsobereflectedbythemediasessionmodalUI.
Additionally,theDiscordteamisexploringmorelong-termsolutionswheretheMLSgroup
membershipstatewouldbedirectlyreflectedbytheclientUI. TOB-DISCE2EE-
7:Keyfingerprintverificationisvulnerabletopartialpreimageattacks
Resolved.ThefingerprintverificationUIwilluseaQRcodeforautomaticverificationand word-
basedfingerprintsasamanualfallback. hasheye 32DiscordDAVEProtocolCryptographicDesignReview PUBLIC

TOB-DISCE2EE-8:Abusereportingmechanismisvulnerabletomessageforgery
Partiallyresolved.Thesectiononabusereportinginthedesigndocumentationnowclearly
statesthatadesignbasedonmessagefrankingshouldbepreferredaslongastheimpacts
onbandwidthandstoragearenegligible.However,theabusereportingmechanismwillnot
bepartoftheinitialreleaseoftheprotocol,accordingtotheDiscordteam.Sincethe
detailsaroundthedesignofthisfeaturewerenotdeterminedatthetimeofthefixreview,
thisissueisconsideredpartiallyresolved. TOB-DISCE2EE-
9:Secureframesencryptionprovidesweakenedforwardsecrecy guarantees
Resolved.ThesecureframesprotocolnowusesanMLSsecrettreeinitializedusingthe exporter_secret
keytoderivesymmetricencryptionkeys. TOB-DISCE2EE-10:Secureframesmayfailtoencrypt AV1-
encodedmediaframes Resolved.AllOBUpayloadsarenowencryptedindependentlyoftheirpositionwithinthe
frame. TOB-DISCE2EE-11:Videoframeheaderlengthandheaderdataarenotauthenticated
Resolved.Allunencrypteddatafromtheframewillnowbeincludedasadditionaldatafor theAEAD. hasheye
33DiscordDAVEProtocolCryptographicDesignReview PUBLIC

D.FixReviewStatusCategories
Thefollowingtabledescribesthestatusesusedtoindicatewhetheranissuehasbeen sufficientlyaddressed.
FixStatus StatusDescription UndeterminedThestatusoftheissuewasnotdeterminedduringthisengagement.
UnresolvedTheissuepersistsandhasnotbeenresolved.
PartiallyResolvedTheissuepersistsbuthasbeenpartiallyresolved.
ResolvedTheissuehasbeensufficientlyresolved. hasheye 34DiscordDAVEProtocolCryptographicDesignReview
PUBLIC