

## 20211109 Ragnarok Security Findings

Date	Contract	Status	Discovery	Issue
2021-12-17	BulletLoans	Fixed	Code reviewing specs	repay() can update state and succeed despite unsuccessful funds transfer().
2021-12-17	ManagedPortfolio	Fixed	Writing specs	Transfers can bypass KYL signature check.
2021-12-21	BulletLoans	Fixed	Running specs	repay() can change DEFAULTED status
2021-12-22	BulletLoans	Fixed	Running specs	markLoanAsDefaulted() can change FullyRepaid and Resolved statuses
2021-12-28	BulletLoans	Fixed	Code reviewing specs	updateLoanParameters() does not update loan status
2022-01-05	ManagedPortfolio	Fixed	QA debugging	Possible reentrancy in deposit
2022-01-05	SignatureValidator	Won't Fix (Ragnarok)	QA debugging	any untrusted contract can bypass the non-US citizen ringfence to deposit into the portfolio
2022-01-05	frontend	Reported	QA debugging	frontend should not always ask lenders for unlimited approval (see Badger DAO hack)
2022-01-05	frontend (MetaMask)	Reported	QA debugging	ECDSA signature should be modified to end in 0x1b or 0x1c instead of 0x00 or 0x01
2022-01-06	ManagedPortfolio	Won't Fix (Ragnarok)	Code reviewing specs	Transfers to a portfolio with zero totalSupply can result in locked funds.
2022-01-10	ManagedPortfolio	Fixed	Running specs	createBulletLoans() repaymentAmount can be less than principal amount
2022-01-11	ManagedPortfolio	Fixed	Running specs	createBulletLoans()/illiquidValue() duration can be zero
2022-01-12	ManagedPortfolio	Fixed	Code reviewing	updateLoanParameters() is never called by ManagedPortfolio
2022-01-16	BorrowerSignature	Won't Fix (Ragnarok)	Direct code analysis	a manager can override a later negotiated set of loan params with an earlier set of loan params without getting a new signature from the borrower
2022-01-18	SignatureValidator	Won't Fix (Ragnarok)	Direct code analysis	deposits from Gnosis Safes and other wallet contracts may not be supported due to EIP-1271 implementation
2022-01-22	ManagedPortfolio	Fixed	Code reviewing specs	updateLoanParameters does not check portfolio endDate
2022-01-22	ManagedPortfolio	Fixed	Code reviewing specs	updateLoanParameters does not update latestRepaymentDate