Grin Security

Process Updates // Audit Review // New Repo // Future Work

@joltz (keybase)
@j01tz (github)
A709 43BD 1098 58B5 034E 23AC 9969 F570 C2EF 616F

QTUM

SPARK POOL

Security Process Update: RFC-003

- Motivation
  - Learn from previous incidents (zcash, bitcoin etc.)
  - Clear and standardized disclosure process
  - Ecosystem resiliency with bi-lateral disclosure agreements
- Open problems
  - Bug bounties
  - Centralization risks weighted against on-chain minimalism
  - Specification vulnerability disclosure

Security Audit #2 Review

- Auditor: Coinspect
- Scope
  - Grin core crate
  - Grin keychain crate
  - Grin chain crate
  - Grin wallet crate*

Security Audit #2 Review

- Timeline:
  - **October 2018** - *Security audit funding campaign begins*
  - **December 2018** - *Security audit funding campaign completed, 16 BTC goal is met*
  - **February 2019** - *Coinspect conducts audit*
  - **February 2019** - *CVE-2019-9195 is reported and fixed*
  - **March - July 2019** - *All findings are investigated and fixed*
  - **August - September 2019** - *Remediation verification period to ensure fixes are correct*
  - **October 2019** - *Publication of findings*

Security Audit #2 Review

- Findings Summary:
  - Critical: 1 (CVE-2019-9195)
  - High: 5
  - Medium: 7
  - Low: 1

Security Audit #2 Review

- General Issues Found
  - Directory traversal and file handling *(CVE-2019-9595)*
  - Unsafe code in third-party libraries *(croaring)*
  - Improperly handled errors in Rust *(panics)*
  - P2P connection logic *(inbound vs outbound connections)*
  - Insufficient validation *(orphan blocks)*
- Possible Impact
  - DoS, data corruption, privilege escalation

Security Audit #2 Review

- Review of CVE-2019-9595
- Timeline
  - **February 22** - *responsible disclosure by Coinspect*
  - **February 25** - *fix released with v1.0.2, CVE assigned*
  - **February 26** - *limited disclosure to mining pools and exchanges*
  - **March 5** - *Public disclosure*

Security Audit #2 Review

- Review of CVE-2019-9595
- Technical Details
  - “Zip Slip”: a directory traversal vulnerability during zip extraction process when synchronizing
    - Attacker provides malicious zip to syncing victim node
    - Victim node extracts zip with directory traversal file names
    - Attacker can overwrite executable/config files and call remotely (or wait for user to trigger)

Security Audit #2 Review

- Review of CVE-2019-9595
- Fix Details: sanitize, skip, whitelist
  - Detect invalid paths and skip corresponding zip files
  - Use whitelist of expected data to filter extracted files

Security Audit #2 Review

- Review of CVE-2019-9595
- Summary
  - Low technical complexity
  - High impact
  - Caught early
  - These kind of bugs are why audits are important
    - Cheap to exploit, not hard to find, high impact

Security Audit #2 Review

- What went well?
- What could be improved?
- Was it worth it?
- Is it sustainable to do this regularly for Grin?

Grin-Security Repo

- PGP Keys
- Canaries + Signatures
- CVEs
- Audits

Future Work

- Build on foundations of RFC-003
  - Foster bi-lateral disclosure agreements
  - Encourage healthy security culture for ecosystem developers and users
- Improve security tooling and integration
- Explore sustainability models for ongoing security work
- Big picture: making Grin secure for use in the real world
  - This includes privacy and usability awareness

https://github.com/mimblewimble/grin-security