大規模マシンを使用した脆弱性調査の進捗について

情報科学類3年　上木亮平

自己紹介

- 情報科学類3年
- こんなものが好きです
  - セキュリティ全般
  - Confidential Computing
    - TEE/CVM
    - Intel TDX/SGX, AMD SEV-SNPなど
  - Anti-Cheat
  - ハイパーバイザー
    - Hyper-V
    - BitVisorなどのthin-HV
    - (Paravisor)
  - ブロックチェーン

本題

脆弱性調査のためのマシン運用をしています

構成

- CPU: Intel Xeon E5-2630 v4 2.20GHz × 2ソケット
- メモリ: 128GB
- ストレージ: SSD 128GB

これが2台あります

- 最近は主にブロックチェーンを構成しているプロトコルの脆弱性調査を行っています
  - 攻撃のE2Eでの実証のためにはある程度大きな計算資源が必要
  - 例えば、あるプロトコルにおけるvalidatorマシン(Consensusを構成するマシン)の推奨最低要件は
    - 24コア
    - RAM 128GB
    - 4TB NVMe
    - (ネットワーク 1Gbps)

- 資金窃取や、署名の検証ミスなどはリソースに関係なく起こり得るが、ノードを落とす/Consensusの形成を進められなくなる脆弱性の証明には本番環境に近いスペックが求められる
  - 例えば、OOMによってノード用のプロセスを落とされることを証明するためには、128GB近くまでプロセスが肥大化することを実証する必要がある
  - 検証のためのスペックが足りない場合は実証できる最大限の大きさで実施し、残りはコード上/数学的に起こり得るということを伝えるしかない
  - が、もちろんできるだけ大きなリソースで実施した方が良い
    - 攻撃を防ぐ、見落としている何かブロッカーがあるかもしれない

実際に却下された例

The PoC demonstrates a crash only under [redacted] — a setup that does not reflect default RPC node hardware. Real [redacted] full nodes are specified to run on 1 TB NVMe storage, so the ENOSPC condition that triggers the panic would not occur at the demonstrated transaction rate.

「このPoCでクラッシュが実証されたのは、〜。
これは、標準的なRPCノードのハードウェア構成を反映したものではありません。
実際のフルノードは1TBのNVMeストレージ上で稼働するよう規定されているため、
パニックを引き起こすENOSPC（ディスク容量不足）の状態は、
実証されたトランザクション処理レートでは発生しません。」

- こういう強いマシンを家に置いて運用するというのは一人暮らし1Kにおいてはかなり非現実的である

- 同じく、脆弱性調査の一環としてKVM/Hyper-Vに対するファジングを行っているが、これももちろん家ではほぼ不可能である

- 上記の理由により実際に学生が自由にマシンを置ける環境が必要とされている

成果

- 複数のプロトコルに対して脆弱性の報告を行った
  - まだレビュワーのトリアージ待ちのものもあるが、実際にスコープ内として脆弱性が確認されたものも複数ある
  - 具体的には、
    - 誤ったコントラクト状態をネットワーク全体で正式に確定させる
    - ネットワーク上のすべてのvalidatorノードで取引の確定を長時間止められる
  - など
  - 特に、後者のようなDoSの検証には現在運用しているようなCPUが強いマシンが必須だった

今後の展望

- より強いマシンを用意して、調査を継続/拡大させていきたい
- ファジングもフルで回せるようになりたい
- もし資金に余裕ができれば、TDXが使用できるマシンを用意して Confidential Computingに対する脆弱性調査も行なってみたい

- 検証用のマシンを貸してくれている間瀬太陽くんにこの場を借りて感謝をしたいです
  - 頭が上がりません
    - Heads Down!
  - 本当にありがとうございます

- ご清聴ありがとうございました