4A-02

新規仮想化ソフトウェアのセキュア実装に向けた既存実装の脆弱性分類の検討

葛野 弘樹 †
神戸大学 大学院工学研究科 †

深井 貴明 ‡
国立研究開発法人 産業技術総合研究所 ‡

1 はじめに

仮想化ソフトウェアの脆弱性は，計算機基盤のメモリ不正改ざんや動作停止に繋がる攻撃に利用される可能性がある．脆弱性の影響を最小化するため，セキュリティを高めた設計とプログラミング言語を用いた仮想化ソフトウェアが開発されている [1]．しかし，ハードウェア制御を伴うソフトウェアの場合，セキュリティを高めた設計を確実に反映した実装は難しく，過去に指摘された種類の脆弱性が含まれる可能性が指摘されている [2]．そのため，新規仮想化ソフトウェアのセキュア実装のために次の目的をあげる．

研究目的 ：脆弱性分析と修正状況の利活用
仮想化ソフトウェアに含まれる過去の脆弱性を整理し，機能毎に分類，脆弱性の傾向と脆弱性修正状況を把握する．今後，新規仮想化ソフトウェアの各機能におけるセキュリティを高めた設計に基づいた実装を実現するための利活用に繋げることを目的とする．

本稿では，既存の仮想化ソフトウェアの脆弱性情報の分析と分類を通じ，脆弱性種別を集約し，分類を行う．また，カーネルの仮想化機能を調査対象とし，脆弱性一覧と脆弱性分類を行い，傾向を把握可能とする．調査において，脆弱性情報は National Vulnerability Database（NVD）を利用し，仮想化ソフトウェアは Linux KVM を対象に脆弱性を分類し把握，新規仮想化ソフトウェアのセキュア実装に利活用可能か検討した．

図 1 調査手順の概要

2 調査方針と手順

2.1 方針

仮想化ソフトウェアの脆弱性分析の方針は次の通りである．

方針：既存の仮想化ソフトウェアにて報告された脆弱性について，脆弱性種別を分析し，分類可能とする．

2.2 手順

調査手順の概要を図 1 に示す．本研究では，NVD の脆弱性データベースから脆弱性情報の一覧を取得し分析対象とする．また，脆弱性の分類指標である 共通脆弱性タイプ一覧 CWE（Common Weakness Enumeration）を用い，脆弱性を種別ごとに分類する．仮想化ソフトウェアは Linux KVM を対象とし， NVD に含まれる Linux KVM の脆弱性を抽出，CWE 毎に分類し，脆弱性の傾向を把握する．

3 調査結果

3.1 調査項目と目的

本研究での調査項目と内容を以下に示す．

Classification of virtual machine monitor vulnerability for secure design and implementation of VMM
† Hiroki Kuzuno, Kobe University
‡ Takaaki Fukai, National Institute of Advanced Industrial Science and Technology

表 1　Top CWE of Linux KVM

Type	Content	CVE
NVD-CWE-noinfo	Insufficient Information	16
CWE-20	Improper Input Validation	13
CWE-476	NULL Pointer Dereference	11
CWE-399	Resource Management Errors	10
CWE-264	Permissions, Privileges, and Access Controls	7
CWE-119	Improper Restriction of Operations	6
CWE-362	Race Condition	6
CWE-416	Use After Free	5
CWE-189	Numeric Errors	4
CWE-200	Exposure of Sensitive Information	4
CWE-787	Out-of-bounds Write	4
17 CWEs	Under 3 CVEs	29
Total		115

- 既存の仮想化ソフトウェアの脆弱性分類
  カーネルの仮想化機能を対象とし，脆弱性収集と分類が可能か調査した．

調査対象

調査対象の脆弱性データベースは NVD より提供されている 2009 年から 2022 年 12 月の json ファイルとした．また，調査対象の仮想化ソフトウェアは，Linux レポジトリにおける KVM ディレクトリに対する 2022 年 12 月までの git log のコミット履歴とした．

3.2　仮想化ソフトウェアの脆弱性分類

調査より, NVD に登録されている Linux KVM に関する脆弱性は 115 件あり，28 種類の CWE が確認された．CWE 毎の脆弱性数を表 1 に示す．表 1 より，10 件以上の CVE が分類された CWE は NVD-CWE-noinfo，CWE-20，CWE-476，CWE-399 であることが確認された．また, CWE に基づく脆弱性の分類結果を図 2 に示す．一部の CWE を補完することで，全体として 10 種類の脆弱性種別が確認された．

4　考察

仮想化ソフトウェアに関する脆弱性は分類可能であり脆弱性の種別を把握可能なことを確認した．表 1 より，上位の脆弱性種別として，入力処理は 13 件，ポインタ参照は 11 件と，入出力や変数の取扱いに関する脆弱性が多い．また，図 2 より，CWE を補完することで複数の脆弱性を同一の種別として捉えることが可能である．新規仮想化ソフトウェアのセキュア実装のためには，脆弱性の種別を容易に一覧し，ソースコード単位での脆弱性修正前後の情報の提示が必要といえる．CWE 情報がない脆弱性もあり，脆弱性単位および仮想化ソフトウェアの個別機能ごとに更なる調査が必要と考えている．

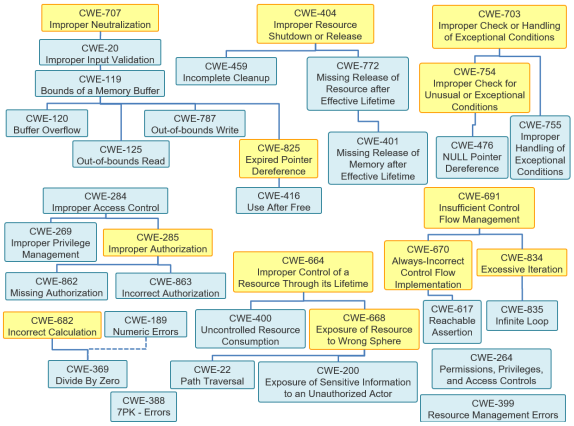

図 2　Linux KVM に関する脆弱性の CWE 分類図

5　まとめと今後の予定

本稿では，仮想化ソフトウェアに関する脆弱性種別を調査，分類し，新規仮想化ソフトウェアのセキュア実装への利活用のために脆弱性傾向を把握可能なことを示した．今後，仮想化ソフトウェアの脆弱性の分類結果を活用し，新規仮想化ソフトウェアのセキュア実装に繋げるため，仮想化機能単位での脆弱なソースコードの指摘や情報提供を検討している．

謝辞

本研究の一部は，JST さきがけ JPMJPR22PB の支援，2022 年度国立情報学研究所公募型共同研究（22S0302）の助成を受けたものです．

参考文献

[1] MilvusVisor, available from `https://github.com/RIKEN-RCCS/MilvusVisor/`. (accessed 2022-11-12).

[2] Bae, Y., et al.: RUDRA: Finding Memory Safety Bugs in Rust at the Ecosystem Scale. *Proc. the ACM SIOPS 28th Symposium on Operating Systems Principles*, October, pp. 84–99, (2021).