毛利研究室輪講資料　令和 4 年度 第 10 回　令和 4 年 12 月 16 日（金）

Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits

山下 恭平

概要：本稿は 31st USENIX Security Symposium にて掲載された論文「Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits」[1] の内容についてまとめたものである. 既存の脆弱性評価基準の分析を通じて得られる結果は, その脆弱性が悪用されることを予測するのには不十分であるため, ソフトウェア脆弱性の公開時の悪用可能性を評価することは困難である. さらに,「悪用できない」という評価は不確実性が高く, 悪用可能性の評価にはバイアスがかかっていることが問題として挙げられる. これらの問題を解決するために, 機能的なエクスプロイトが開発される可能性を経時的に反映する,Expected Exploitability（EE）と呼ばれる新しい指標を提案する.

1. はじめに

エクスプロイトがセキュリティに深刻な影響を与えた事例として,2017 年に世界中で大流行した WannaCry と NotPetya がある. これらが悪名高い成功を納めた原因として, 武器化されたエクスプロイトの使用が挙げられる. しかし, 武器となり得る脆弱性を利用するプログラムを開発する難易度が上がっていることから, 既知の脆弱性のうち 5%のみを悪用することに注力するようになっている. そういった中で, 着目すべき脆弱性の優先順位をつけることで人々に対して最適な意思決定をもたらし, 悪用防止に向けた研究機会の深い理解のために, 各脆弱性の悪用可能性を評価する必要がある. しかし, 悪用可能性の評価は, どの脆弱性が, どのように利用されるかが不明なため, 困難である. 具体的には,WannaCry や NotPetya によって悪用された脆弱性である CVE-2017-0144 は, 当時の専門家が推奨するパッチから省かれたいた. このことから, エクスプロイトの開発によってエクスプロイト可能性を証明することはできるが, 非エクスプロイト可能性を証明することは困難である. この結果,「悪用不可能」という評価にはバイアスが発生し, 不確実性を持つことが分かる.

この問題を解決するために Expected Exploitability (EE) と呼ばれる新しい指標を提案する. この指標は, 脆弱性を「悪用可能」または「悪用不可能」と決定的に分類するのではなく, 類似の脆弱性に関する過去のパターンに基づいて, 機能的なエクスプロイトが開発される可能性を時系列で継続的に推定するものである. ここで機能的なエクスプロイトとは, 脆弱性が引き起こすセキュリティ上の問題を完全に実現するものであり, 機能的なエクスプロイトは実際の攻撃を容易にする. この論文の目的は機能的なエクスプロイトが開発されることを予測するのが目的である.

2. 問題の概要

エクスプロイトの開発によって, 悪用可能性を証明することができるが, 悪用不可能であることを証明するのは困難である. その代わりに, 脆弱性悪用緩和の取り組みとして, 悪用の難しさを把握する目的とした脆弱性スコアリングシステムがよく用いられる. 以下にその例をあげる.

- NVD CVSS[2]
  - 必要なアクセス制御, 攻撃ベクトルの複雑さ, 権限レベルなど, 様々な脆弱性の特性を 0〜4 の値に落とし込んだもの.4 が最も悪用可能性が高い.
- Microsoft Exploitability Index[3]
  - Microsoft が 0〜3 の 4 段階で悪用可能性を評価し割り当てる,Microsoft 固有のスコア.
- RedHat Severity[4]
  - CVSS を補完し,RedHat 製品に影響を与える脆弱性について専門家の評価によって, 同様に脆弱性の悪用の難易度を評価したもの.

しかし, これらのベンダーなどから提供される指標は, 不正確であることが報告されている. 具体的な事例として,Internet Explorer の悪用可能な脆弱性である CVE-2018-8174 は,CVSS 悪用可能性スコア 1.6 を獲得し, 脆弱性スコアの 91%以下に位置づけられた. 同様に,Windows7 から 10 に影響を及ぼす悪用される脆弱性である CVE-2018-8440 は, スコアが 1.8 とされた.

3. 課題

4. 収集するデータ

5. 評価

6. おわりに

参考文献

[1] Octavian Suciu , Connor Nelson , Zhuoer Lyu , Tiffany Bao , and Tudor Dumitras. Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits. In 31th USENIX Security Symposium (USENIX Security 22), pages 377-394, 2022

[2] A complete guide to the common vulnerability scoring system. `https://www.first.org/cvss/v3.0/specification-document` . (15/12/2022)

[3] Microsoft exploitability index. Microsoft. `https://www.microsoft.com/en-us/msrc/exploitability-index` . (15/12/2022)

[4] Severity Rating. RedHat. `https://access.redhat.com/security/updates/classification/` . (15/12/2022)