6ZC-03

COVID-19 前後における脆弱性情報と攻撃プログラム公開までの時間差に生じた変化

牧野 千穂† 丸山 一貴‡

明星大学 情報学部 情報学科† 明星大学 情報学部 情報学科‡

1. はじめに

ソフトウェアやプログラムに脆弱性が発見されると，図 1 の流れで対応が行われる．CVE は脆弱性情報，CVE-ID はその識別番号である．エクスプロイトはパッチリリースの前後，CVE 公開後のいずれかのタイミングで発生する[1]．CVE として詳細な情報が公開されると，脆弱性の内容に応じて CVSS(Common Vulnerability Scoring System) という脆弱性深刻度スコアがつけられる．スコアはいくつかの基準を用いて算出される．

先行研究として，CVE の公開日からエクスプロイトの公開日までの期間(以下，ディレイ期間という．)と CVSS の評価基準を分析し，非常に短い期間でエクスプロイトが作成されている評価指標の組み合わせが存在することがわかっている[2]．しかし，データは 2018 年 6 月までのものを利用しており，COVID-19 によってリモートワークが増えてからの期間は調査されていない．

本研究は 2018 年 7 月から 2022 年 7 月までのエクスプロイトを追加して，COVID-19 前後での評価基準の組み合わせによるディレイ期間に変化があるか，調査・分析することを目的とする．

2. 関連研究

Roumani[3]はゼロデイ脆弱性に対するパッチリリースについて，CVSS の評価が与える影響を分析した．また，Shahid ら[4]は BERT を利用した分類器を用いて CVSS の深刻度予測を行った．ゼロデイ脆弱性と自然言語処理によるスコア予測の研究は存在する．しかし，本研究ではゼロデイ脆弱性は取り扱わずに，ディレイ期間を用いて分析を行う．

3. 提案手法

本研究では Exploit Database[1]と NVD(National Vulnerability Database)[2]を用いてデータの抽出を行う．Exploit Database からはエクスプロイトの公開日と対応する CVE-ID を利用する．対応する CVE-ID が存在しないものは分析の対象外とする．NVD からは CVE-ID と公開日，CVSS の評価指標を利用する．また，ディレイ期間がゼロデイを示すものと，それぞれの公開日が同日の場合は対象外としている．

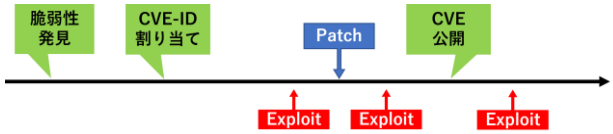

図 1:エクスプロイトが公開されるタイミング[1]

各データは CVE-ID を用いて紐づけを行う．取り扱うデータは先行研究と同様に NVD 設立の 2005 年 8 月から，Exploit Database のデータ抽出の際に利用したファイルの更新日である 2022 年 7 月までである．分析に利用するパラメータは CVSS の基本評価指標のみである。基本評価指標は，CVSS の評価指標の中でも環境に左右されない脆弱性の特性を表すものである．CVSS には v2 と v3 という異なるバージョンが存在するが，先行研究と同様に v2 の値を v3 に対応させている．v3 の各指標を 1 から 4 種類の組み合わせにし，ディレイ期間を集計，中央値を算出した．各期間の結果と全体の中央値などを比較して分析を行う．なお，基本評価指標の組み合わせは先行研究にならって，攻撃元区分，攻撃条件の複雑さ，ユーザ関与レベル，機密性への影響に限定した．

表 1:ディレイ期間の中央値と 80 パーセンタイルの変化(単位:日)

期間	中央値	80 パーセンタイル
2005 年 8 月から 2018 年 6 月	29	291.6
2018 年 7 月から 2019 年 12 月	10	133
2020 年 1 月から 2022 年 7 月	14	91

The change of vulnerability exploit delay through COVID-19
†Chiho Makino, Department of Information Science, School of Information Science, Meisei University
‡Kazutaka Maruyama, Department of Information Science, School of Information Science, Meisei University

表 2:ディレイ期間に大きな変化が見られた組み合わせ(単位:日)

CVSS 評価指標	データ数 2005/8~ 2018/6	中央値 2005/8~ 2018/6	データ数 2018/7~ 2019/12	中央値 2018/7~ 2019/12	データ数 2020/1~ 2022/7	中央値 2020/1~ 2022/7
攻撃元区分:Network 攻撃条件の複雑さ:Low ユーザ関与レベル:Required 機密性への影響:Low	106	3	120	6	210	9
攻撃元区分:Network 攻撃条件の複雑さ:Low ユーザ関与レベル:None 機密性への影響:High	807	34	223	26	442	15

4. 分析結果

2018 年 7 月から 2019 年までの対象データ数が 607 件, 2020 年以降の対象データ数が 884 件である. それぞれの期間におけるディレイ期間の中央値と 80 パーセンタイルをまとめたのが表 1 である. 2018 年 7 月から 2019 年 12 月までの中央値が一番短くなっているが, 80 パーセンタイルを比較してみると全体の傾向としては徐々に短くなっていることがわかる. 表 2 は集計したデータから特に変化が大きいと考えられるデータを抜粋している. 1 つ目の評価の組み合わせは COVID-19 前後で期間が延びており, データ数が増加している例である. 2 つ目は中央値が大きく短縮されている例を挙げている.

5. 考察

表 1 から COVID-19 後のデータとしてディレイ期間が全体を通して短縮傾向にあることがわかる. 表 2 では 2 つの例として, ネットワークから攻撃可能で攻撃が比較的簡単に行え, ユーザのアクションが必要で機密性への影響が低い攻撃は期間が若干延びている傾向がある. 逆にユーザのアクションが不要で, 機密性への影響が高い組み合わせにおいて, 期間が非常に短縮されていることが分かった. 2 つで全く異なる変化が見られた. 労力をできるだけ使わずに, より多くの機密情報を得られるような脆弱性を対象としたエクスプロイト開発が優先されている可能性がある.

6. まとめ

本研究ではエクスプロイトの公開日と CVE の公開日を用いることで CVE とエクスプロイトの CVSS に関する COVID-19 の前後における傾向を分析した. 結果, 指標によって大きく変化がみられる組み合わせが存在し, COVID-19 の前後でエクスプロイト開発の優先度に変化が表れている可能性が考えられた. 今後はこれらの組み合わせに共通する脆弱性の特徴について詳細に調べ, 具体的にどの脆弱性に対する攻撃が増加しているのかを調査していく.

参考文献

[1] A. Feutrill, D. Ranathunga, Y. Yarom and M. Roughan,“The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay”, 2018 Sixth International Symposium on Computing and Networking(CANDAR), pp.1-10, doi: 10.1109/CANDAR.2018.00009.

[2] Jay Chen, エクスプロイトの開発状況:80%のエクスプロイトは CVE より先に公開されている, <https://unit42.paloaltonetworks.jp/state-of-exploit-development/>,(参照 2022/12/25)

[3] Yaman Roumani, “Patching zero-day vulnerabilities: an empirical analysis”, Journal of Cybersecurity, Vol.7, Issue 1, 2021.

[4] M.R. Shahid, H. Debar, “CVSS-BERT: Explainable Natural Language Processing to Determine the Severity of a Computer Security Vulnerability from its Description”,2021 20th IEEE International Conference on Machine Learning and Applications(ICMLA), pp.1600-1607, 2021, doi: 10.1109/ICMLA52953.2021.00256.

[1]https://www.exploit-db.com/
[2]https://nvd.nist.gov/