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

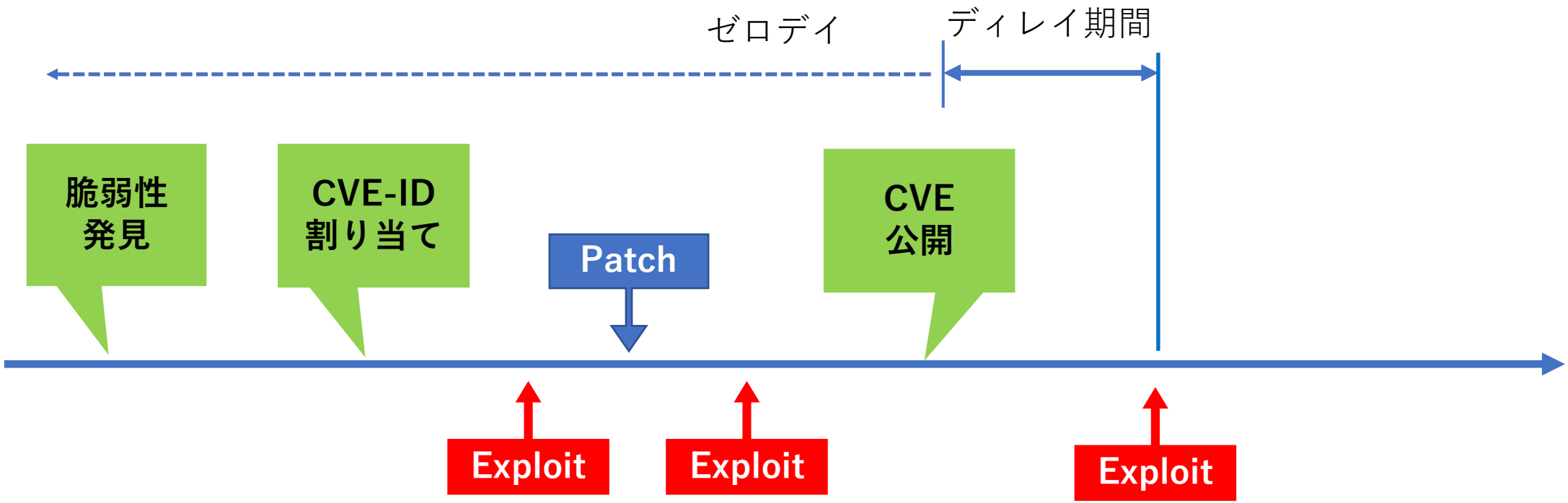
2022年度 明星大学 情報学部 情報学科

丸山研究室

19J5-125 牧野千穂

背景

エクスプロイト・パッチ・CVE公開日の関係[2]



エクスプロイト:攻撃プログラム　CVE:脆弱性情報

CVEとは

- CVE-ID
- 脆弱性詳細
- データ作成日等

Printer-Friendly View

CVE-ID	
CVE-2020-1003	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0913, CVE-2020-1000, CVE-2020-1027.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1003	
Assigning CNA	
Microsoft Corporation	
Date Record Created	
20191104	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20191104)	
Votes (Legacy)	
Comments (Legacy)	

CVEとは

- CVE-ID
- 脆弱性詳細
- データ作成日等

Printer-Friendly View

CVE-ID	
CVE-2020-1003	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0913, CVE-2020-1000, CVE-2020-1027.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1003

Assigning CNA

Microsoft Corporation

Date Record Created

20191104	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20191104)

Votes (Legacy)

Comments (Legacy)

CVEとは

- CVE-ID
- 脆弱性詳細
- データ作成日等

Printer-Friendly View

CVE-ID	
CVE-2020-1003	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0913, CVE-2020-1000, CVE-2020-1027.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1003

Assigning CNA

Microsoft Corporation

Date Record Created

20191104	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20191104)

Votes (Legacy)

Comments (Legacy)

CVEとは

- CVE-ID
- 脆弱性詳細
- データ作成日等

Printer-Friendly View

CVE-ID	
CVE-2020-1003	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0913, CVE-2020-1000, CVE-2020-1027.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1003

Assigning CNA

Microsoft Corporation

Date Record Created	
20191104	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

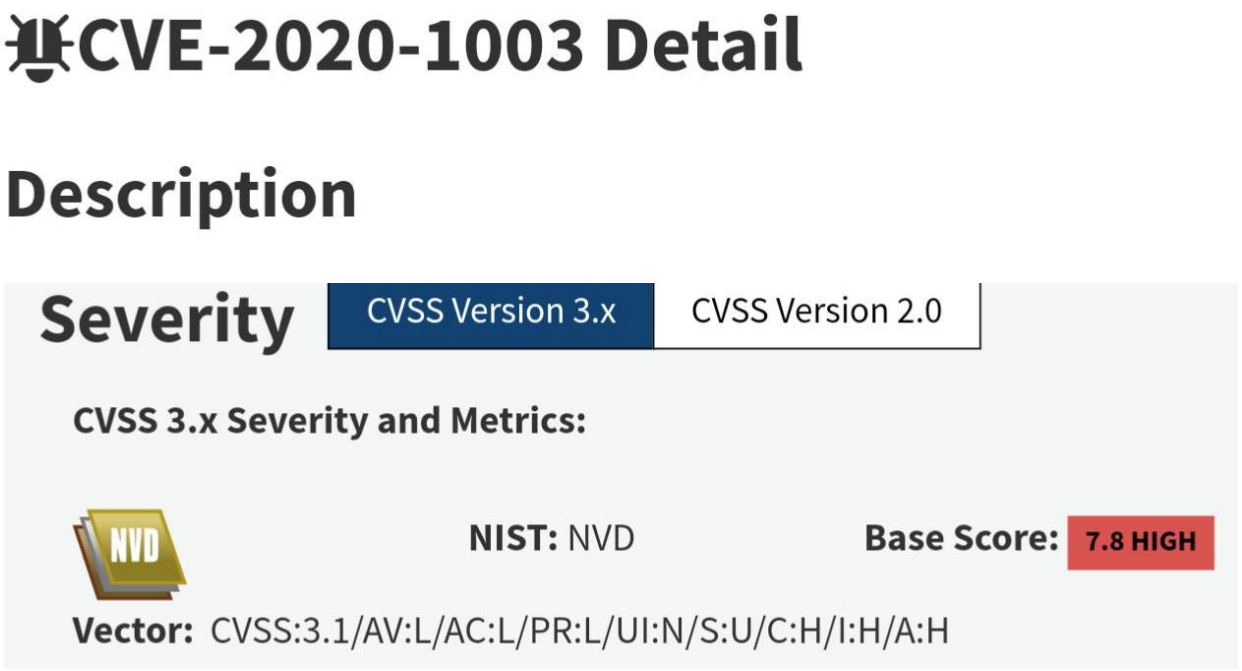
Assigned (20191104)

Votes (Legacy)

Comments (Legacy)

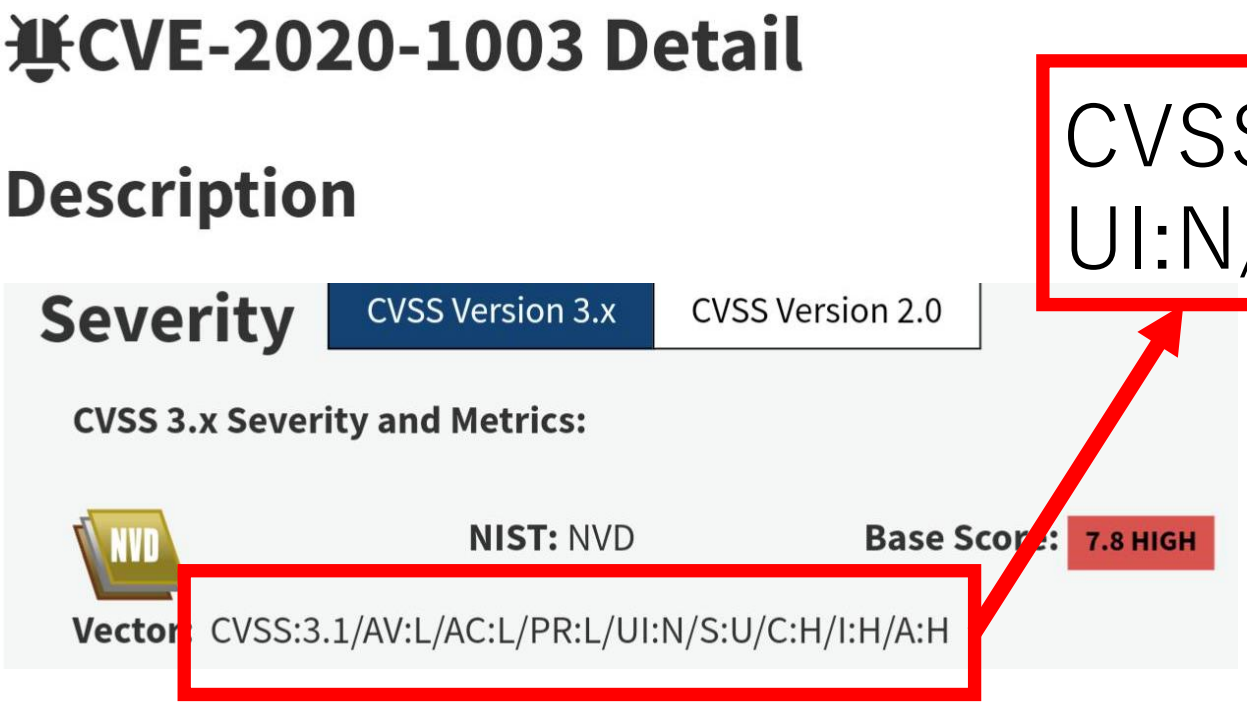
CVSSとは

- Common Vulnerability Scoring System
- NVD(National Vulnerability Database)で公開されている脆弱性深刻度



CVSSとは

- Common Vulnerability Scoring System
- NVD(National Vulnerability Database)で公開されている脆弱性深刻度



CVSS:3.1/AV:L/AC:L/PR:L/
UI:N/S:U/C:H/I:H/A:H

基本評価指標

目的

- ディレイ期間とCVSSの基本評価指標で分析
- 先行研究では2018年7月以降は未分析
- COVID-19前後での変化を調査
- セキュリティ対策での優先順位付けへの応用

関連研究(1)

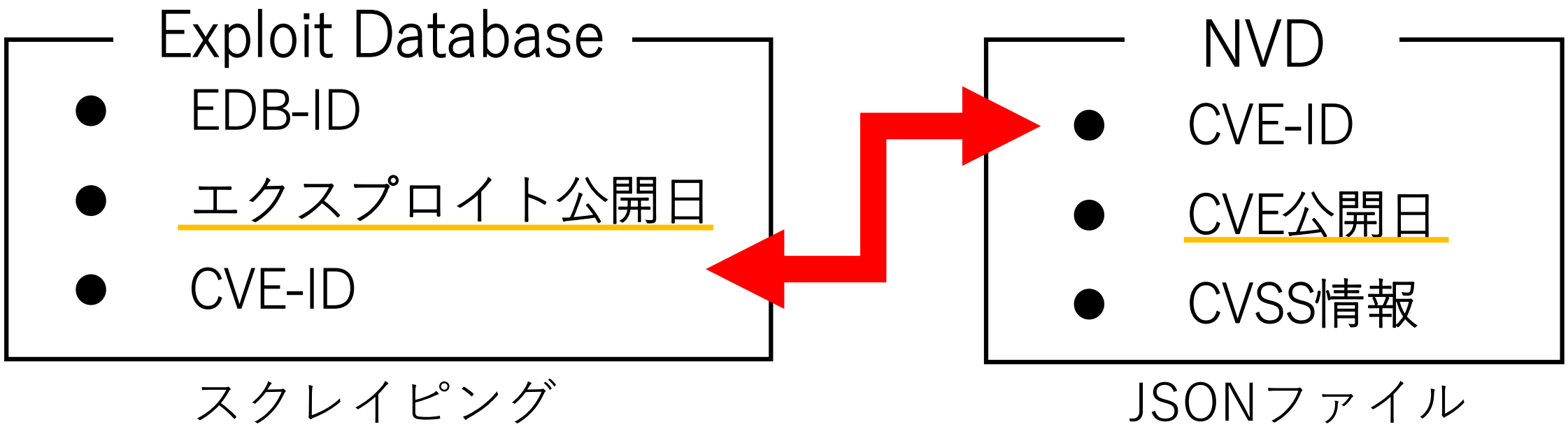
- Feutrillら[1]
  - ExploitDBを利用して2005年8月から2018年6月までのエクスプロイトについて調査
  - CVSSの特定の組み合わせにおいてディレイ期間の短縮

CVSS指標	評価	データ数	中央値(日)
Attack Complexity Attack Vector Confidentiality Impact User Interaction	Low Network Low Required	95	5

関連研究(2)

- Roumani[3]
  - パッチリリースまでの時間に影響を与える要素について調査
  - 深刻度が高いものはパッチリリースを遅延させる可能性が高い
- 山越ら[4]
  - 運用担当者の役割や環境を考慮した脆弱性診断システム
  - CVSS等を利用

提案手法(1)



ディレイ期間＝エクスプロイト公開日 ー CVE公開日

提案手法(2)

- 期間を3つに分割
- 2005年8月から2018年6月までを再集計
- 再集計データの比較

実装

期間ごとにデータを抽出

CVSSの評価の組み合わせを全て取得

各組合せを持つデータを集計

データ数・中央値を算出

分析結果・考察(1)

期間	データ数	中央値	80 percentile	最大値
2005/08～2018/06	3778	29	291.6	5635
2018/07～2019/12	607	10	133	1036
2020/01～2022/07	884	14	91	820

単位:日

- COVID-19前の中央値が最短
- 全体を通してディレイ期間の短縮

分析結果・考察(1)

期間	データ数	中央値	80 percentile	最大値
2005/08～2018/06	3778	29	291.6	5635
2018/07～2019/12	607	10	133	1036
2020/01～2022/07	884	14	91	820

増 減

単位:日

- COVID-19前の中央値が最短
- 全体を通してディレイ期間の短縮

分析結果・考察(2)

CVSS評価指標	2005/08～2018/06 データ数	2005/08～2018/06 中央値(日)	2018/07～2019/12 データ数	2018/07～2019/12 中央値(日)	2020/01～2022/07 データ数	2020/01～2022/07 中央値(日)
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

分析結果・考察(2)

CVSS評価指標	2005/08～2018/06 データ数	2005/08～2018/06 中央値(日)	2018/07～2019/12 データ数	2018/07～2019/12 中央値(日)	2020/01～2022/07 データ数	2020/01～2022/07 中央値(日)
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

結論

- ネットワークから攻撃可能
- 攻撃が複雑でない
- ユーザの認証が不必要
- 機密性への影響が高い

上記の脆弱性についてエクスプロイト開発が優先されている可能性

今後の課題

- 特定の組み合わせにおけるディレイ期間が短縮されている脆弱性の詳細を調査
- COVID-19前後におけるリモートワークの関連性の有無
- より細かい期間に分割した分析

- 情報処理学会第85回全国大会発表予定