セミナー資料 配布版

ICT-ISAC セミナー　オープンセミナー　2023

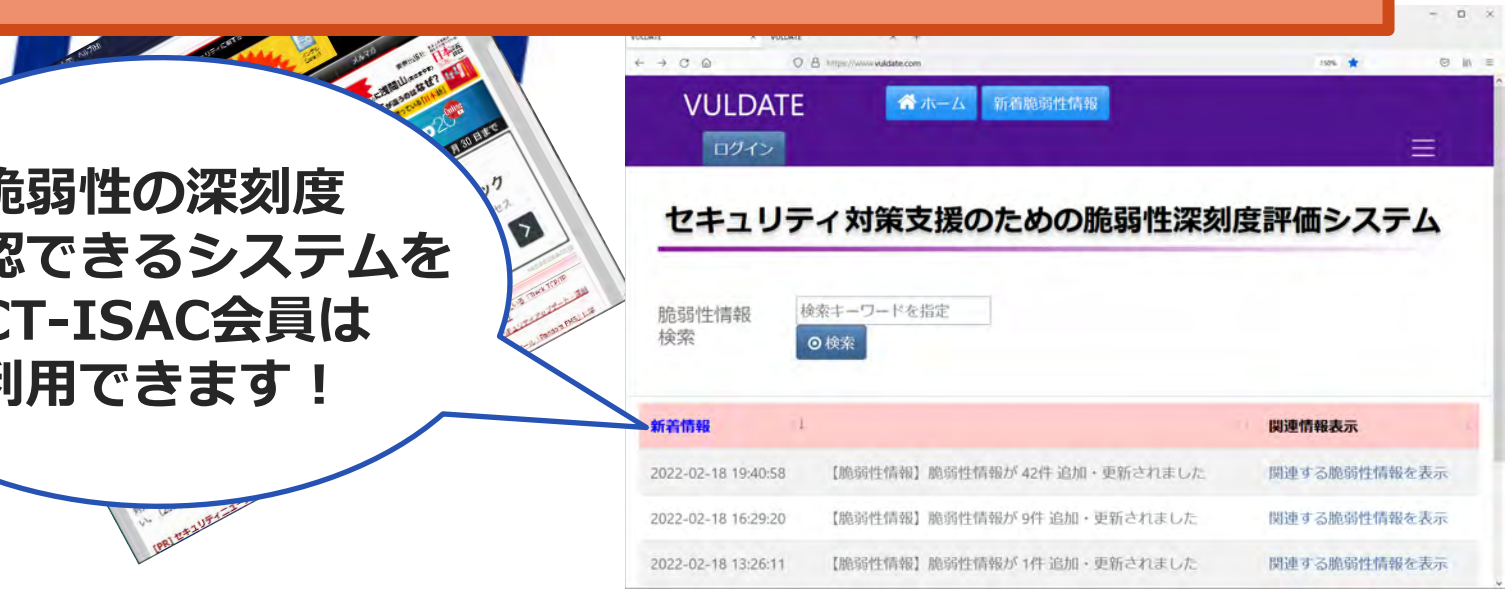
「脆弱性深刻度評価システム(Vuldate)による実用的な脅威影響評価」

KDDI総合研究所
サイバーセキュリティグループ

2023年3月3日

本日の内容

深刻なサイバー攻撃による被害への対策

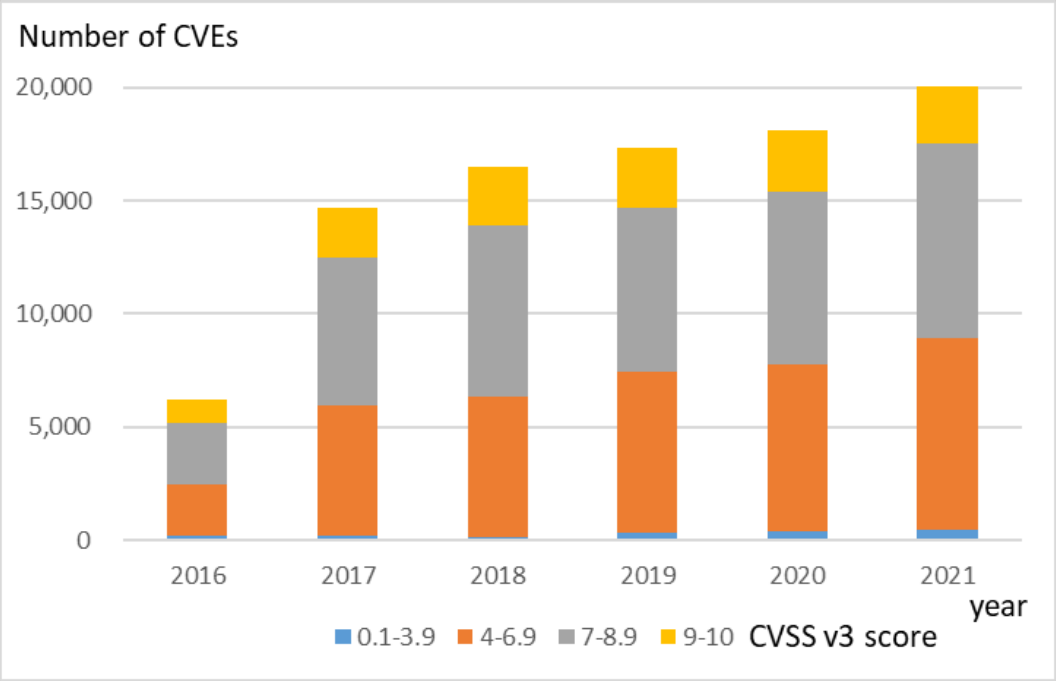


脆弱性とは

- 脆弱性
  - コンピューターネットワークにおける安全上の欠陥。ソフトウェア上のバグやハードウェアの欠陥に乗じて、悪意のある第三者により不正アクセスや、マルウェアへの感染などの被害が生じる可能性があること。
    情報セキュリティ・サイバーセキュリティの用語で安全上の欠陥を指す。

Log4j

脆弱性件数



- 20,000件/年以上報告される脆弱性
- CVSSのスコアが高い（7-10）ものだけでも、2000件以上/年

CVE：Common Vulnerabilities and Exposures
◆共通脆弱性識別子
～脆弱性の固有ID

CVSS：Common Vulnerability Scoring System
◆共通脆弱性評価システム
～脆弱性の深刻度評価の仕組み

脆弱性対策の進め方　～脆弱性情報の収集～

A

■ 脆弱性や脅威に関する情報を入手

出典
IPA Technical Watch脆弱性対策の効果的な進め方（実践編）第２版
図2-2-2：情報収集のイメージ図

- 対策にあたり沢山の情報を収集しなくてはならない
- 参照すべきサイトも沢山ある

コスト大
（人的コスト、etc.）

脆弱性対策の進め方　脆弱性情報の分析

■ 脆弱性情報の危険度の分析

脆弱性の危険度を分析

脆弱性A ＞ **脆弱性B** ＞ **脆弱性C**

？

参考
IPA Technical Watch脆弱性対策の効果的な進め方（実践編）第２版
図2-2-1：情報収集から分析までのイメージ図

■ 脆弱性の特徴など、各種情報・状況からその脆弱性の危険度を確認

■ 対象であるか、対処すべき脆弱性であるかの判断

■ セキュリティに関する知識・専門性が必要

■ 組織によって事情が異なる

Vuldateについて

Vuldateの役割

脆弱性情報に関して・・・・・

脆弱性の**関連情報を確認**：
「VuldateがWebから収集した情報や類似事例」を確認

脆弱性対応の優先度付けの支援：
「Vuldateが分析評価した深刻度の指標」を利用

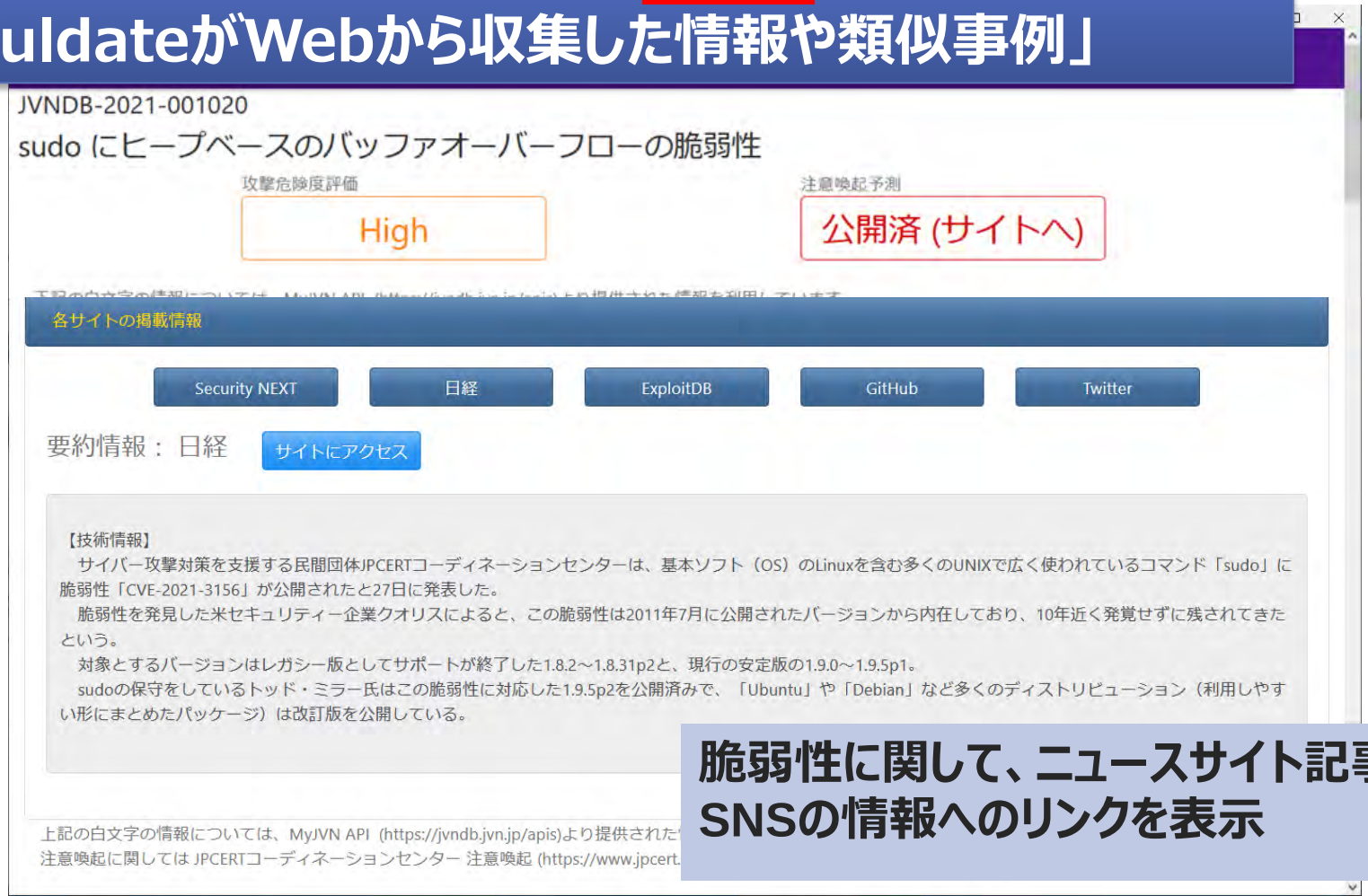
Vuldateによる情報収集支援

脆弱性の関連情報を確認：
「VuldateがWebから収集した情報や類似事例」を確認

- 報告された脆弱性に関して、Web上を検索し、ニュース記事の要約を表示
- 関連する情報のニュースサイト、SNSサイトのリンクを提示

情報収集の労力を削減

脆弱性の関連情報を確認：　画面例
「VuldateがWebから収集した情報や類似事例」



脆弱性に関して、ニュースサイト記事の要約やSNSの情報へのリンクを表示

VULDATE

JVNDB-2021-001020

sudo にヒープベースのバッファオーバーフローの脆弱性

攻撃危険度評価

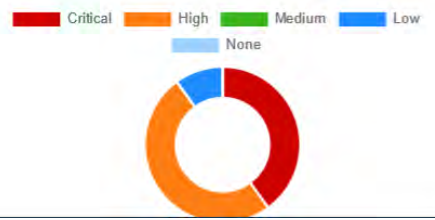
High

注意喚起予測

公開済 (サイトへ)

JVNDB-2017-001848	Commvault Edge にスタックバッファオーバーフローの脆弱性	High
JVNDB-2016-007716	McAfee Virus Scan Enterprise for Linux に複数の脆弱性	Low
JVNDB-2017-002402	Microsoft OLE URL Moniker における遠隔の HTA データに対する不適切な処理	High
JVNDB-2017-013150	Apple iOS および macOS のセキュリティコンポーネントにおける XPC メッセージの送信の制限を回避される脆弱性	High
JVNDB-2016-006096	Mozilla Firefox における解放済みメモリ使用 (use-after-free) の脆弱性	High

当該の脆弱性の類似の脆弱性とその危険度を提示



Vuldateによる脆弱性情報分析

脆弱性対応の優先度付けの支援：
「Vuldateが分析評価した深刻度の指標」を利用

- 報告された脆弱性に関して、機械学習を用いて、その深刻度を評価
- 攻撃危険度評価（攻撃コードが生成される危険性）と注意喚起予測（注意喚起に相当するような脆弱性かどうか）を判断

優先度付けの指標を参考に

実際に攻撃コードが観測された脆弱性の割合

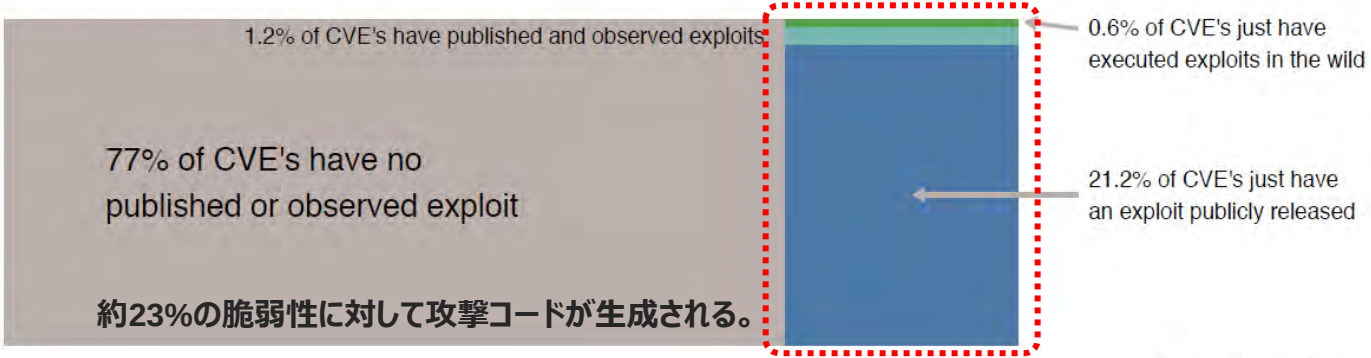
■ 攻撃コードの生成

- 攻撃コードが利用されると実際に被害が生じ、インシデントにつながる
- すなわち、攻撃コードが生成されそうな脆弱性の対処の優先度が高い
- 但し、脆弱性のすべてに攻撃コードが生成されるわけではない。

攻撃コードが生成される脆弱性を見極める

FIGURE 2

Comparison of CVEs with exploit code and/or observed exploits in the wild relative to all published CVEs



約23%の脆弱性に対して攻撃コードが生成される。

Source: Kenna / Cyentia

注意喚起の活用

■ 注意喚起とは？

- セキュリティに関わる団体やベンダーが，発覚した脆弱性や脅威，攻撃による被害状況等を把握し，危険性の高い脆弱性やサイバー攻撃に対して注意を促すもの
- システム管理者は、注意喚起をきっかけにセキュリティ対策を見直すきっかけにもなり、対応すべき脆弱性の優先度付けに必要な情報の一つ

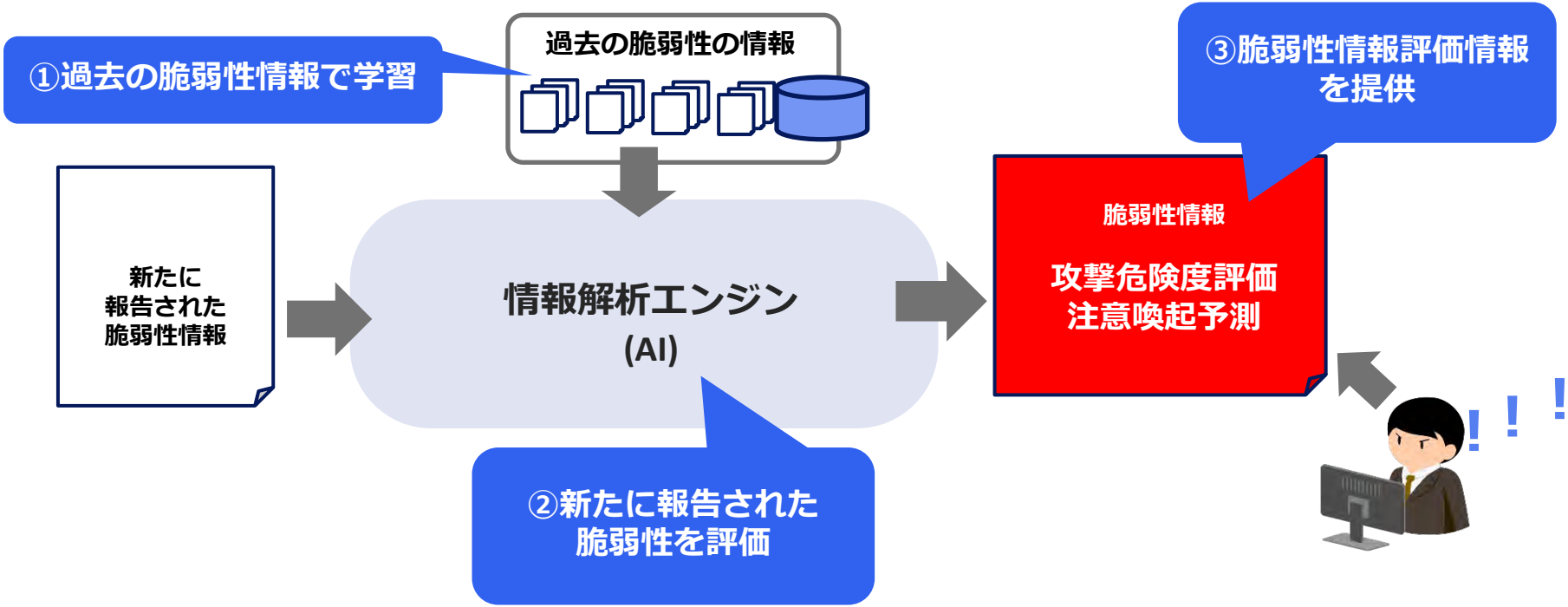
注意喚起になるような脆弱性は深刻度が高い

出典：JPCERT/CC 注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

AIによる脆弱性情報分析

■ 機械学習の活用

- “攻撃コードが生成されるか”、“注意喚起に相当するか”を分析
- 機械学習を用いることで、人的コストの削減を実現



Vuldateの使い方（参考）

A

ニュースサイト

NEWS

Vuldate

脆弱性情報
（評価値）

SNS

公表値

CVSS値

自社の
資産

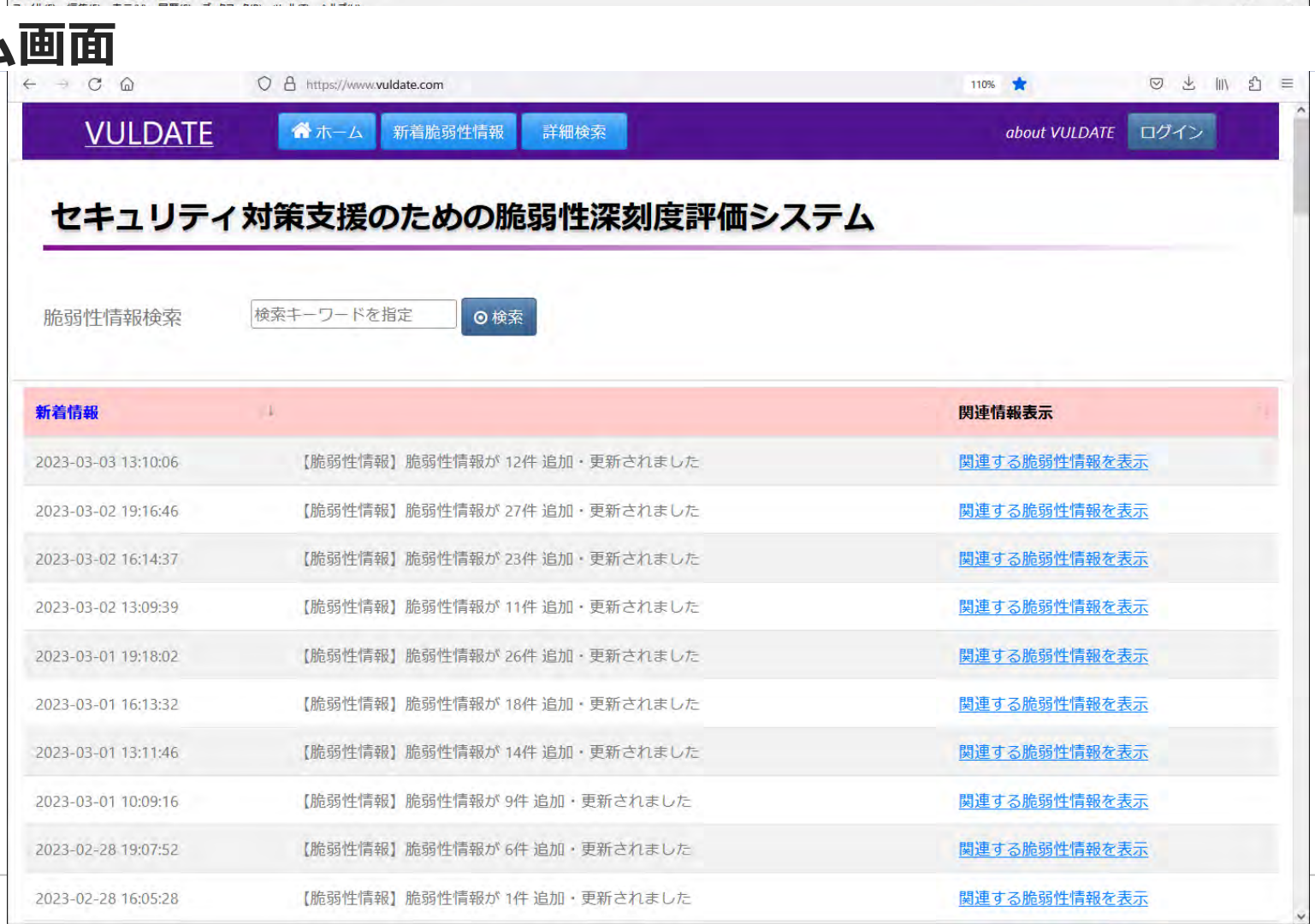
多様の情報により判断・社内への連絡

Vuldateのサービス提供

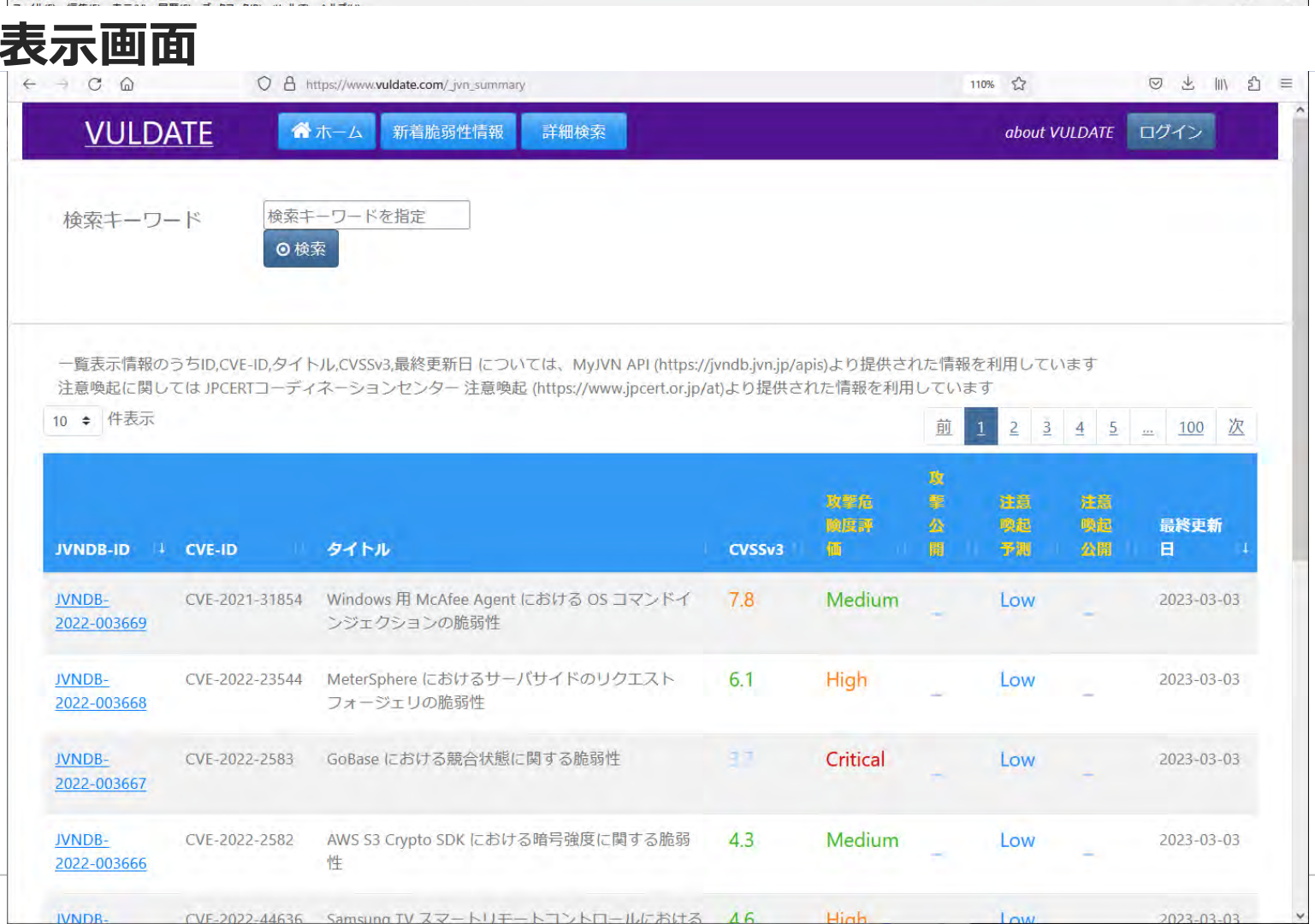
ICT-ISAC会員向けサービスとして提供中

- 希望する会員に無償提供
- 20＋の組織に提供中
- 2022年度にアップデートを実施

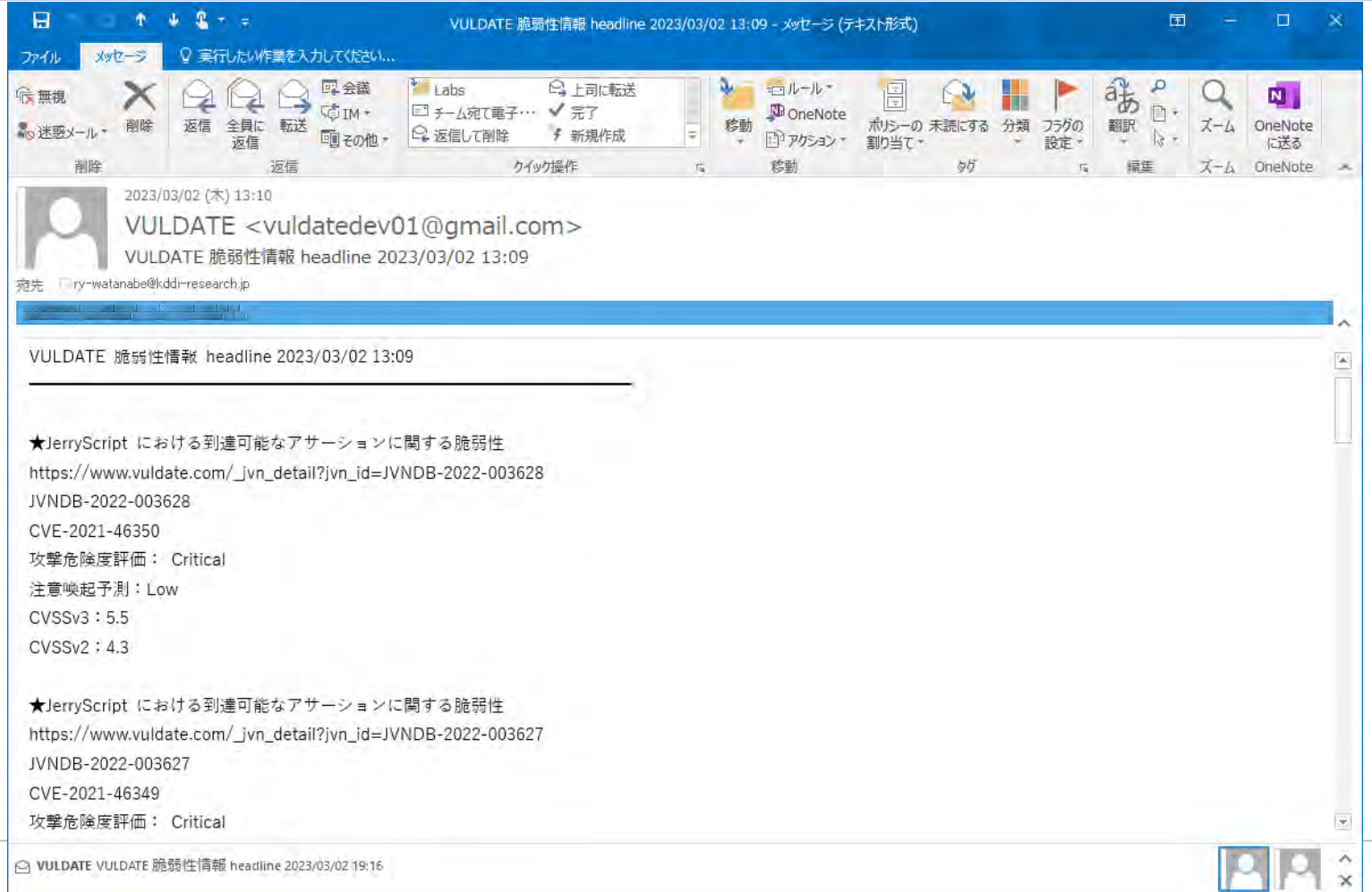
システム画面


https://www.vuldate.com
110%
VULDATE
ホーム
新着脆弱性情報
詳細検索
about VULDATE
ログイン
セキュリティ対策支援のための脆弱性深刻度評価システム
脆弱性情報検索
検索キーワードを指定
検索
新着情報
関連情報表示
2023-03-03 13:10:06 【脆弱性情報】脆弱性情報が 12件 追加・更新されました 関連する脆弱性情報を表示
2023-03-02 19:16:46 【脆弱性情報】脆弱性情報が 27件 追加・更新されました 関連する脆弱性情報を表示
2023-03-02 16:14:37 【脆弱性情報】脆弱性情報が 23件 追加・更新されました 関連する脆弱性情報を表示
2023-03-02 13:09:39 【脆弱性情報】脆弱性情報が 11件 追加・更新されました 関連する脆弱性情報を表示
2023-03-01 19:18:02 【脆弱性情報】脆弱性情報が 26件 追加・更新されました 関連する脆弱性情報を表示
2023-03-01 16:13:32 【脆弱性情報】脆弱性情報が 18件 追加・更新されました 関連する脆弱性情報を表示
2023-03-01 13:11:46 【脆弱性情報】脆弱性情報が 14件 追加・更新されました 関連する脆弱性情報を表示
2023-03-01 10:09:16 【脆弱性情報】脆弱性情報が 9件 追加・更新されました 関連する脆弱性情報を表示
2023-02-28 19:07:52 【脆弱性情報】脆弱性情報が 6件 追加・更新されました 関連する脆弱性情報を表示
2023-02-28 16:05:28 【脆弱性情報】脆弱性情報が 1件 追加・更新されました 関連する脆弱性情報を表示

一覧表示画面


https://www.vuldate.com/_jvn_summary
110%
VULDATE
ホーム
新着脆弱性情報
詳細検索
about VULDATE
ログイン
検索キーワード
検索キーワードを指定
検索
一覧表示情報のうちID,CVE-ID,タイトル,CVSSv3,最終更新日 については、MyJVN API (https://jvndb.jvn.jp/apis)より提供された情報を利用しています
注意喚起に関しては JPCERTコーディネーションセンター 注意喚起 (https://www.jpcert.or.jp/at)より提供された情報を利用しています
10 件表示
前 1 2 3 4 5 ... 100 次
JVNDB-ID
CVE-ID
タイトル
CVSSv3
攻撃危険度評価
攻撃公開
注意喚起予測
注意喚起公開
最終更新日
JVNDB-2022-003669
CVE-2021-31854
Windows 用 McAfee Agent における OS コマンドインジェクションの脆弱性
7.8
Medium
Low
2023-03-03
JVNDB-2022-003668
CVE-2022-23544
MeterSphere におけるサーバサイドのリクエストフォージェリの脆弱性
6.1
High
Low
2023-03-03
JVNDB-2022-003667
CVE-2022-2583
GoBase における競合状態に関する脆弱性
Critical
Low
2023-03-03
JVNDB-2022-003666
CVE-2022-2582
AWS S3 Crypto SDK における暗号強度に関する脆弱性
4.3
Medium
Low
2023-03-03

送信メール

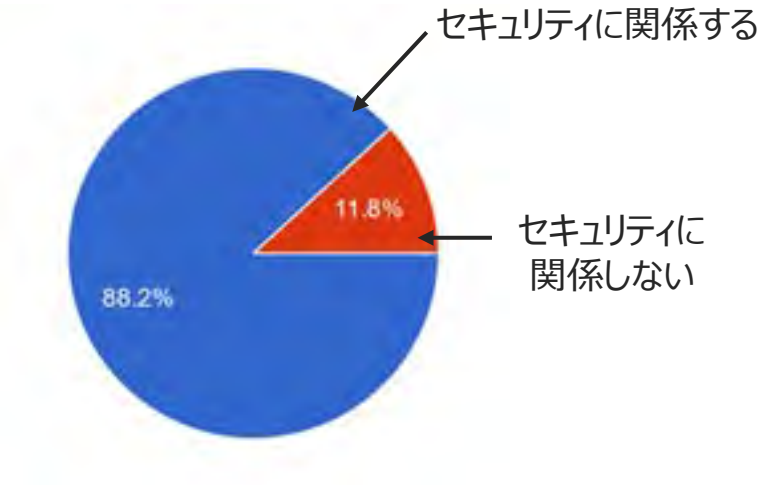

VULDATE 脆弱性情報 headline 2023/03/02 13:09 - メッセージ (テキスト形式)
ファイル
メッセージ
実行したい作業を入力してください...
無視
迷惑メール
削除
返信
全員に返信
転送
会議
IM
その他
Labs
チーム宛て電子…
返信して削除
上司に転送
完了
新規作成
移動
ルール
OneNote
アクション
ポリシーの割り当て
未読にする
分類
フラグの設定
翻訳
ズーム
OneNote に送る
削除
返信
クイック操作
移動
タグ
編集
ズーム
OneNote
2023/03/02 (木) 13:10
VULDATE <vuldatedev01@gmail.com>
VULDATE 脆弱性情報 headline 2023/03/02 13:09
宛先 ry-watanabe@kddi-research.jp
VULDATE 脆弱性情報 headline 2023/03/02 13:09
★JerryScript における到達可能なアサーションに関する脆弱性
https://www.vuldate.com/_jvn_detail?jvn_id=JVNDB-2022-003628
JVNDB-2022-003628
CVE-2021-46350
攻撃危険度評価： Critical
注意喚起予測：Low
CVSSv3：5.5
CVSSv2：4.3
★JerryScript における到達可能なアサーションに関する脆弱性
https://www.vuldate.com/_jvn_detail?jvn_id=JVNDB-2022-003627
JVNDB-2022-003627
CVE-2021-46349
攻撃危険度評価： Critical
VULDATE VULDATE 脆弱性情報 headline 2023/03/02 19:16

Vuldateシステム・ユーザ利用

ユーザアンケート

●利用に関する満足度とニーズ調査のためユーザアンケートを実施
●アンケートでの回答を基に機能更新を実施

◆アンケート回答者の属性



業務内容	対象者
CSIRT	3
内部統制	1
セキュリティ監査	1
セキュリティエンジニア	4
セキュリティ研究者	6
セキュリティに関する企画立案	3
セキュリティ開発者	2
システム運用者	1
セキュリティに関する普及啓発	1
アプリケーション開発者	1
セキュリティに関する技術コンサルタント	1
ISAC	1

ユーザアンケート

Vuldateのインプレッション（抜粋）

新しい試みで期待している。
ニュースサイトやtwitterに情報があるかなどが表示され、ExploitDBやGitHubのページへのリンクがあるのは便利と感じた。
一覧表示において、CVSSに加え「攻撃危険度評価」「攻撃展開予測」が表示されるため、危険性が高い場合、危険な印象を利用者に強く与えることができる。
一覧表示において、表示内容によって色が変わるので、直感的に分かり易い。
ソート機能が早くて快適。
極論ではありますが脆弱性も悪用されなければよいという考え方からすると悪用可能性の評価は非常に重要な取り組みと考えられる。取組につきましては今度も情報をご連携いただけると助かります。
公開された脆弱性情報のうち、悪用可能性について評価された情報は非常に貴重な情報となる。

ユーザアンケート

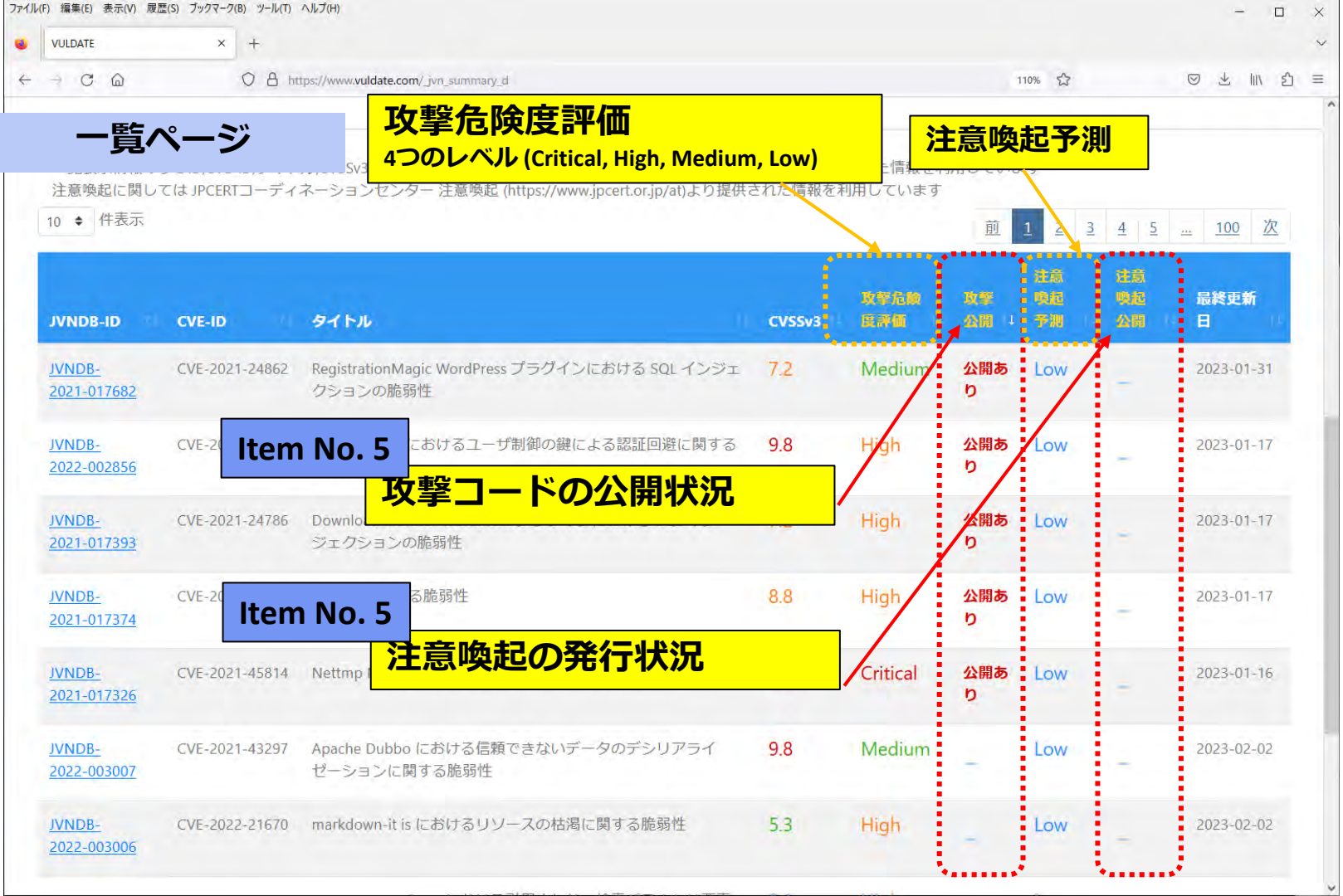
脆弱性評価システムへの要望（抜粋）

最新の分析結果が入手できるように分析希望の対象をインプットできるようにして欲しい
数値や指標で危険というのはなんとなくわかる。加えて、この数値はこんだけ危険であるとわかるような補足が欲しい。
詳細情報（概要等）はデフォルトで表示されているか、または前回の状態を引き継いでいる方がよい。類似事例に記載されているページへのリンクが貼られていると使い勝手がよい。
脆弱性対応には、優先度の根拠（悪用可能性が高いとされる理由）についても情報が求められる。そのため悪用可能性の評価結果に加えその理由が分かる情報も提供されるとよい。
システム所管部の脆弱性管理担当者が使用製品を登録し、登録した製品のみの脆弱性情報を配信する機能があると、対応の正確性、実効性が高まると思われる。
情報の取捨選択が難しい。個人の情報に紐づき、自分自身の業務に関連するものが、もう少し楽にピックアップされるとよい。
脆弱性情報詳細表示で、「各サイトの掲載情報」はソースが固定されている。もっと広いソースから情報を見られるとよい。

2022年度のアップデート

アップデート内容

	No.	内容	リリース	スライド
AI	AI	機械学習の再学習機能	済	–
Web表示	1	トップページに検索機能（検索ウィンドウ）を追加	済	
	2	「攻撃コードの生成」「注意喚起」の状況を別表示	済	○
	3	CVE-IDを詳細画面に追加	済	○
	4	JVN iPedia (JVN-ID) と NVD(CVE-ID)へのリンクを追加	未	
	5	分析結果と「攻撃コード」「注意喚起」の発行状況を個別に表示	済	○
ユーザカスタマイズ	6	詳細画面で表示する項目を指定可能	済	○
	7	関連情報の有無を一覧表示に追加	済	
	8	詳細画面の表示（開閉状況）を保持	済	○
	9	ネットワークの観測情報をメールに追加	済	
	10	攻撃コードが生成済み、注意喚起が発行済みである場合はメールサブジェクトに表示	未	
	11	メールでの通知のレベルを指定可能	済	○
	12	脆弱性情報に対してブックマークを指定可能	未	○



注意喚起に関しては JPCERTコーディネーションセンター 注意喚起 (https://www.jpcert.or.jp/at)より提供された情報を利用しています

10 件表示

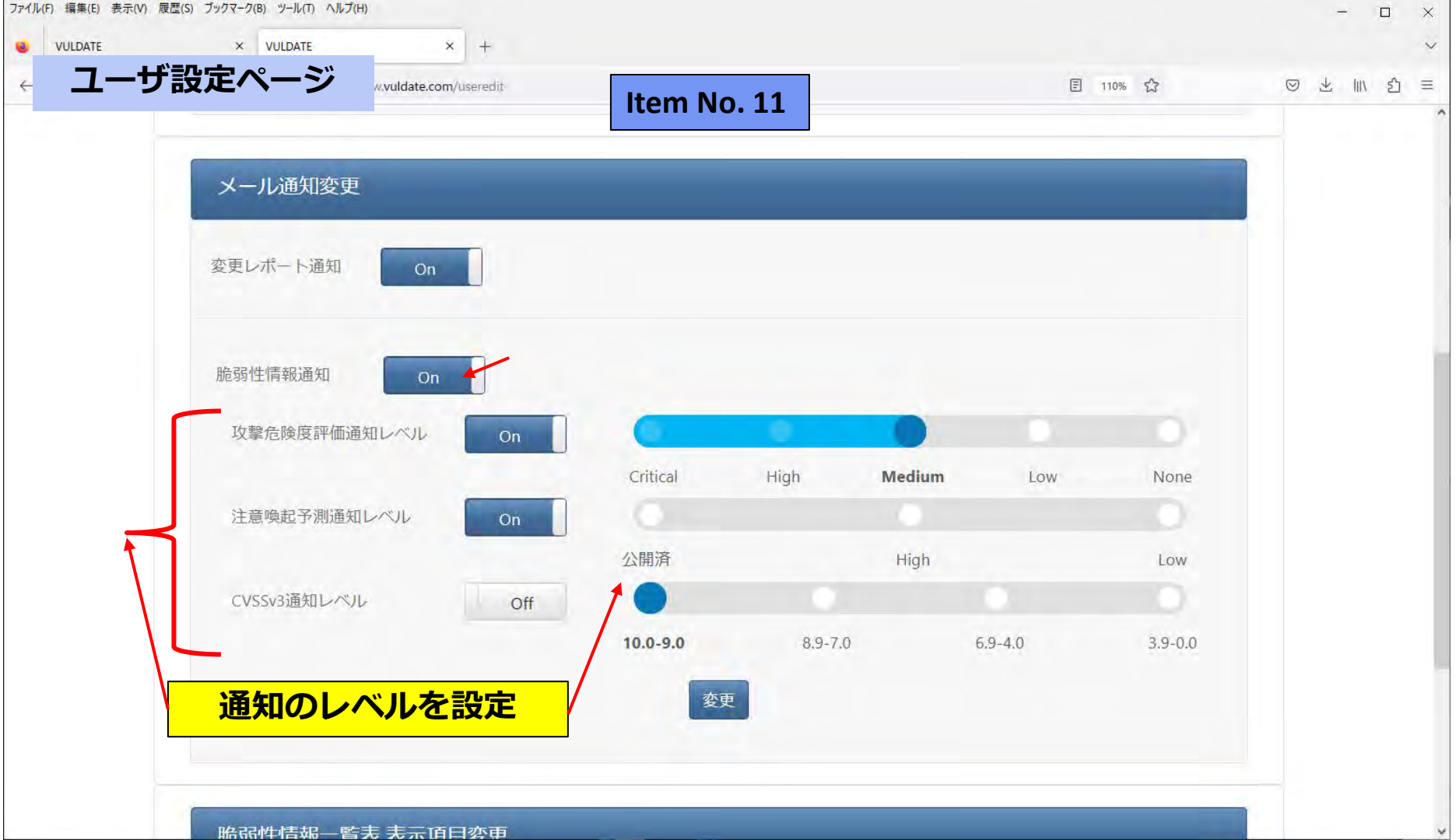
前 1 2 3 4 5 ... 100 次

JVNDB-ID	CVE-ID	タイトル	CVSSv3	攻撃危険度評価	攻撃公開	注意喚起予測	注意喚起公開	最終更新日
JVNDB-2021-017682	CVE-2021-24862	RegistrationMagic WordPress プラグインにおける SQL インジェクションの脆弱性	7.2	Medium	公開あり	Low	-	2023-01-31
JVNDB-2022-002856	CVE-2	におけるユーザ制御の鍵による認証回避に関する	9.8	High	公開あり	Low	-	2023-01-17
JVNDB-2021-017393	CVE-2021-24786	Downlo ジェクションの脆弱性		High	公開あり	Low	-	2023-01-17
JVNDB-2021-017374	CVE-2	る脆弱性	8.8	High	公開あり	Low	-	2023-01-17
JVNDB-2021-017326	CVE-2021-45814	Nettmp		Critical	公開あり	Low	-	2023-01-16
JVNDB-2022-003007	CVE-2021-43297	Apache Dubbo における信頼できないデータのデシリアライゼーションに関する脆弱性	9.8	Medium	-	Low	-	2023-02-02
JVNDB-2022-003006	CVE-2022-21670	markdown-it is におけるリソースの枯渇に関する脆弱性	5.3	High	-	Low	-	2023-02-02


詳細ページ
Item No. 3
CVE-IDを追加
VULDATE
about VULDATE
JVNDB-2022-002856
CVE-2021-45428
TLR-2005KSH におけるユーザ制御の鍵による認証回避に関する脆弱性
攻撃危険度評価
High
攻撃コード公開
公開あり
注意喚起予測
Low
注意喚起公開
注意喚起なし
攻撃コードの公開状況
注意喚起の発行状況
すべて閉じる
影響を受ける製品
Item No. 2
Telesquare
TLR-2005KSH ファームウェア None
概要
TLR-2005KSH には、ユーザ制御の鍵による認証回避に関する脆弱性が存在します。
CVSSによる深刻度
CVSS v3 による深刻度
基本値：9.8
[NVD値] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2 による深刻度
基本値：7.5
[NVD値] AV:N/AC:L/Au:N/C:P/I:P/A:P

ユーザ設定ページ

Item No. 6

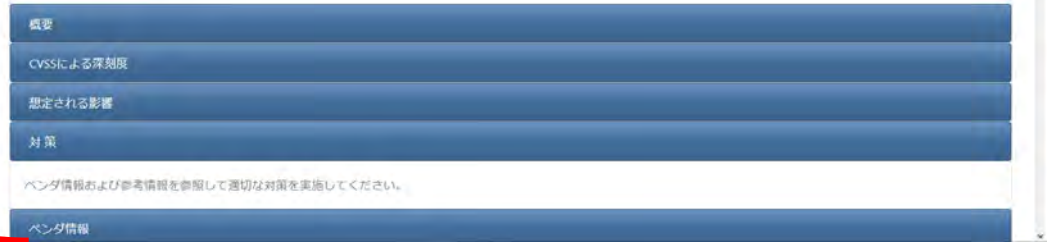

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
VULDATE
VULDATE
ユーザ設定ページ
w.vuldate.com/useredit
110%
Item No. 11
メール通知変更
変更レポート通知
On
脆弱性情報通知
On
攻撃危険度評価通知レベル
On
Critical
High
Medium
Low
None
注意喚起予測通知レベル
On
公開済
High
Low
CVSSv3通知レベル
Off
10.0-9.0
8.9-7.0
6.9-4.0
3.9-0.0
通知のレベルを設定
変更
脆弱性情報一覧表 表示項目変更

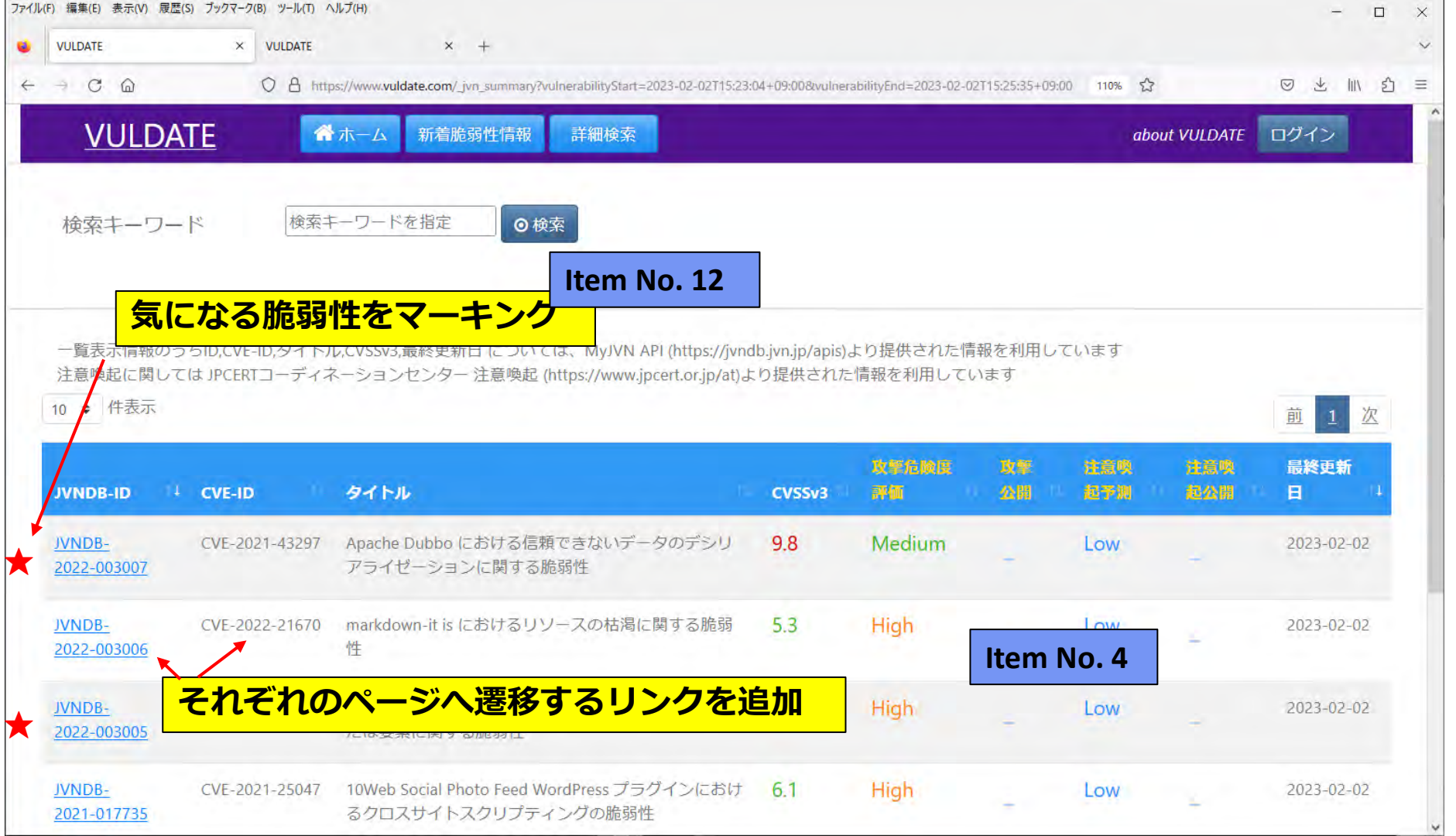
Item No. 8

詳細情報の各項目の開閉状態を保持

Open

Close




VULDATE
ホーム
新着脆弱性情報
詳細検索
about VULDATE
ログイン
検索キーワード
検索キーワードを指定
検索
Item No. 12
気になる脆弱性をマーキング
一覧表示情報のうちID,CVE-ID,タイトル,CVSSv3,最終更新日については、MyJVN API (https://jvndb.jvn.jp/apis)より提供された情報を利用しています
注意喚起に関してはJPCERTコーディネーションセンター 注意喚起 (https://www.jpcert.or.jp/at)より提供された情報を利用しています
10 件表示
前 1 次
JVNDB-ID
CVE-ID
タイトル
CVSSv3
攻撃危険度評価
攻撃公開
注意喚起予測
注意喚起公開
最終更新日
JVNDB-2022-003007
CVE-2021-43297
Apache Dubbo における信頼できないデータのデシリアライゼーションに関する脆弱性
9.8
Medium
Low
2023-02-02
JVNDB-2022-003006
CVE-2022-21670
markdown-it is におけるリソースの枯渇に関する脆弱性
5.3
High
Item No. 4
2023-02-02
それぞれのページへ遷移するリンクを追加
JVNDB-2022-003005
High
Low
2023-02-02
JVNDB-2021-017735
CVE-2021-25047
10Web Social Photo Feed WordPress プラグインにおけるクロスサイトスクリプティングの脆弱性
6.1
High
Low
2023-02-02

運用レポート 2022/06～2023/01

運用に関するレポート

- ●メールの通知頻度は、日に3～4回程度 (サイトビューは、3～4回/週)
- ●よく確認された脆弱性情報は下記
- ●現在の利用者は、OS、アプリの脆弱性に興味がある？

よく参照された脆弱性トップ3

	JVNDB-ID	CVEI-ID	Overview	CVSSv3	Attack code generation score	Security Alert Score	Access Term
1	JVNDB-2021-013667	CVE-2021-30787	Vulnerability in macOS	7.8	High	Low	2022/09 ～2023/01
2	JVNDB-2021-009903	CVE-2021-32012	Resource Exhaustion Vulnerability in SheetJS and SheetJS Pro	5.5	High	Low	2022/08 ～2023/01
3	JVNDB-2021-010495	CVE-2021-20032	Vulnerability in SonicWall Analytics On-Prem	9.8	Critical	Low	2022/07
3	JVNDB-2021-017088	CVE-2021-45623	Command injection vulnerability in several NETGEAR devices	9.8	High	Low	2023/01

よく参照された脆弱性

	JVNDB-ID	CVEI-ID	Overview	説明	対策
1	JVNDB-2021-013667	CVE-2021-30787	Vulnerability in macOS	**macOS における脆弱性** 想定される攻撃： 情報を取得される、情報を改ざんされる、およびサービス運用妨害 (DoS) 状態にされる可能性があります。	ベンダにより対策が公開済み
2	JVNDB-2021-009903	CVE-2021-32012	Resource Exhaustion Vulnerability in SheetJS and SheetJS Pro	**SheetJS および SheetJS Pro におけるリソースの枯渇に関する脆弱性** 想定される攻撃： サービス運用妨害 (DoS) 状態にされる可能性があります。	ベンダにより対策が公開済み
3	JVNDB-2021-010495	CVE-2021-20032	Vulnerability in SonicWall Analytics On-Prem	**SonicWall Analytics On-Prem における脆弱性** 想定される攻撃： 情報を取得される、情報を改ざんされる、およびサービス運用妨害 (DoS) 状態にされる可能性があります。	ベンダにより対策が公開済み
3	JVNDB-2021-017088	CVE-2021-45623	Command injection vulnerability in several NETGEAR devices	**複数の NETGEAR デバイスにおけるコマンドインジェクションの脆弱性** 想定される攻撃： 情報を取得される、情報を改ざんされる、およびサービス運用妨害 (DoS) 状態にされる可能性があります。	ベンダにより対策が公開済み

参照元：JVN iPedia (https://jvndb.jvn.jp/)

まとめ

脆弱性対策の課題：構成管理・構成情報との連携

A

公開情報

社内情報

脆弱性情報
(Vuldate)

資産管理
(構成管理)

部品情報
(SBOM等)

脆弱性情報

攻撃危険度評価
注意喚起予測

これが
難しい・・・

管理する資産との紐づけ

まとめ

■脆弱性深刻度評価システム(Vuldate)の実践的な利用について

- **企業の脆弱性対策を支援するシステム**
  - 実践的な脆弱性対策の実現を支援
  - 脆弱性・脅威に関する情報に加え、資産管理との両輪
- **ICT-ISAC会員向けサービスとして提供中**
  - ご希望する会員は事務局へご連絡下さい

ご清聴ありがとうございました！