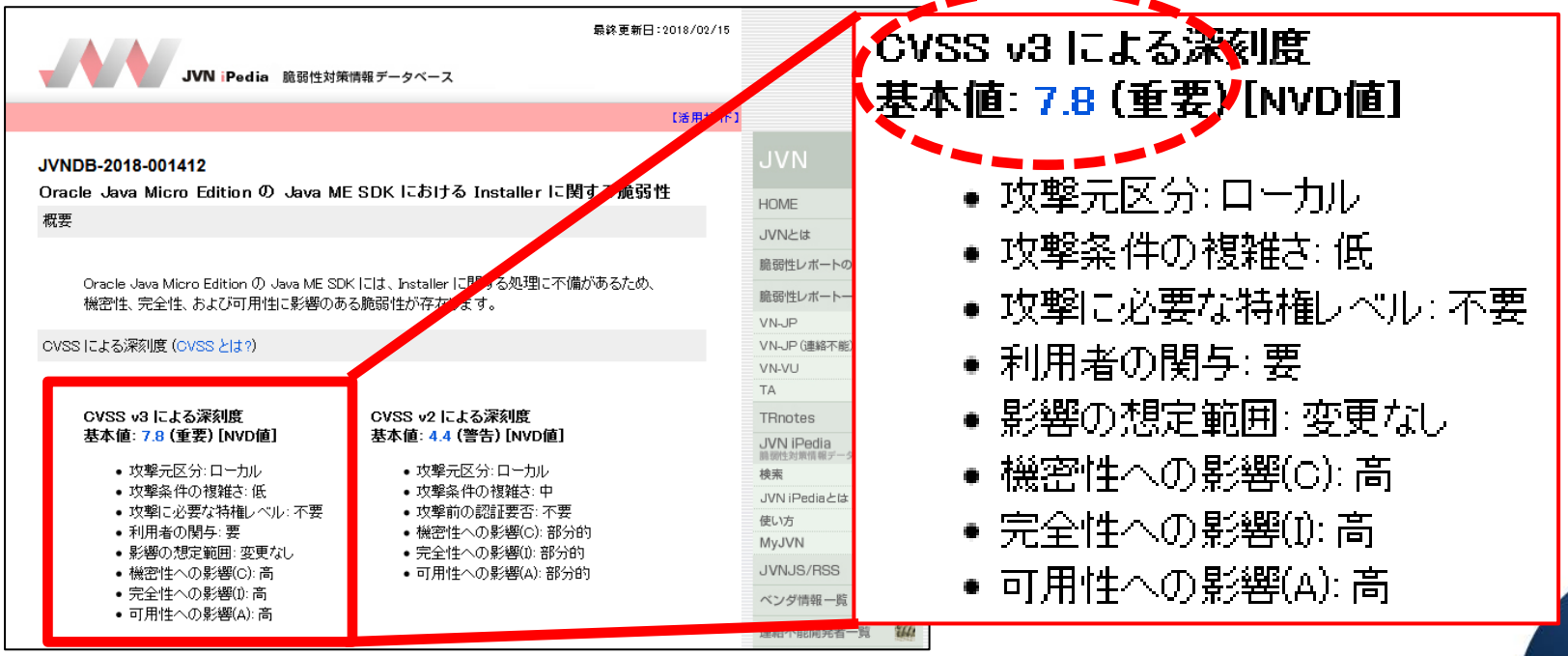
５．IPAの脆弱性対策支援ツール等紹介

脆弱性情報の効率的な収集①

脆弱性対策情報データベース JVN iPedia

https://jvndb.jvn.jp/

- 国内外30,000件以上の製品の脆弱性情報を日本語で提供
- 日付、ベンダ、製品、キーワード等で検索可能
- CVSSに基づく深刻度（CVSS基本値）も記載



必要な情報の効率的な収集②

MyJVN バージョンチェッカ

https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

- PCにインストールされているソフトウェア製品のバージョンが最新のものか、簡単な操作で確認可能

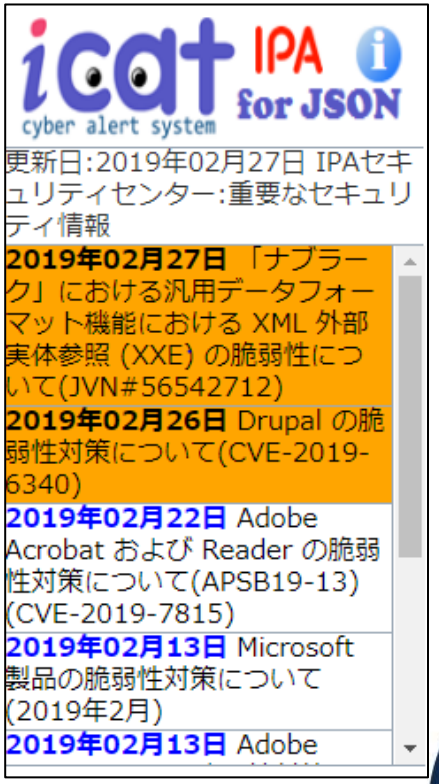
- Adobe Reader、JRE、Google Chrome等、多く利用されている12種類のソフトウェア製品についてチェック可能

必要な情報の効率的な収集③

icat for JSON

https://www.ipa.go.jp/security/vuln/icat.html

- HTMLタグを埋め込むことで、IPAが発信する「重要なセキュリティ情報」を自社のイントラにリアルタイムに表示



- 「重要なセキュリティ情報」は、インターネット利用者に広く影響を及ぼす危険なセキュリティ上の問題が対象
- Microsoft、Adobe、Oracle製品など、企業内でも利用度の高い製品について多く発信

重要なセキュリティ情報とは
https://www.ipa.go.jp/security/security-alert/about.html

必要な情報の効率的な収集④

- **サーバ用オープンソースソフトウェアに関する製品情報およびセキュリティ情報**

  https://www.ipa.go.jp/security/vuln/oss/sw_security_info.html

  -広く利用されているオープンソースソフトウェアのバージョン情報や
  セキュリティ情報を掲載
  -対象ソフトウェア
  Apache Struts,　ISC BIND, Joomla!, OpenSSL, WordPress 等

3.ソフトウェア製品のセキュリティ情報

オープンソースソフトウェアとして提供されている、以下のサーバ用ソフトウェア製品について製品開発者情報および、セキュリティに関する情報を掲載、更新（週1回程度）しています。

Apache HTTP Server	Apache Struts	Apache Tomcat	ISC Bind	Joomla!Japan	OpenSSL	WordPress (日本語)

映像コンテンツのご紹介

■ **本日説明した内容相当の動画をYouTubeでも公開しています**

https://www.youtube.com/playlist?list=PLi57U_f9scIKfSpnABcnhcOHXJ5XZHEuv

他にもIPAではセキュリティに関する映像コンテンツを公開しています

https://www.ipa.go.jp/security/videos/list.html

情報収集先例

注意喚起サイト①

IPA：重要なセキュリティ情報

https://www.ipa.go.jp/security/security-alert/index.html

Microsoft 製品の脆弱性対策について(2024年1月)

公開日：2024年1月10日
最終更新日：2024年1月10日

注釈： 追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

2024年1月10日（日本時間）に Microsoft 製品に関する脆弱性の修正プログラムが公表されています。
これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御されたりして、様々な被害が発生するおそれがあります。

攻撃が行われた場合の影響が大きいため、早急に修正プログラムを適用して下さい。

対策

1.脆弱性の解消 - 修正プログラムの適用

Microsoft 社から提供されている修正プログラムを適用して下さい。
Windows Update の利用方法については以下のサイトを参照してください。

Windows Update の利用手順 – Windows 11 の場合
Windows Update の利用手順 – Windows 10 の場合

参考情報

・2024年1月のセキュリティ更新プログラム（月例）
・セキュリティ更新プログラムガイド
注釈：閲覧には利用規約への同意が必要な場合があります。
・サイバーセキュリティ注意喚起サービス「icat for JSON」

- IPAが公表する注意喚起情報
- マイクロソフト・オラクル・アドビ製品等利用者が多く存在するソフトウェアの脆弱性対策情報を掲載
- 悪用有無を「緊急」「注意」で確認可能

緊急　注意

- 下記サービス・ツールでも入手可能

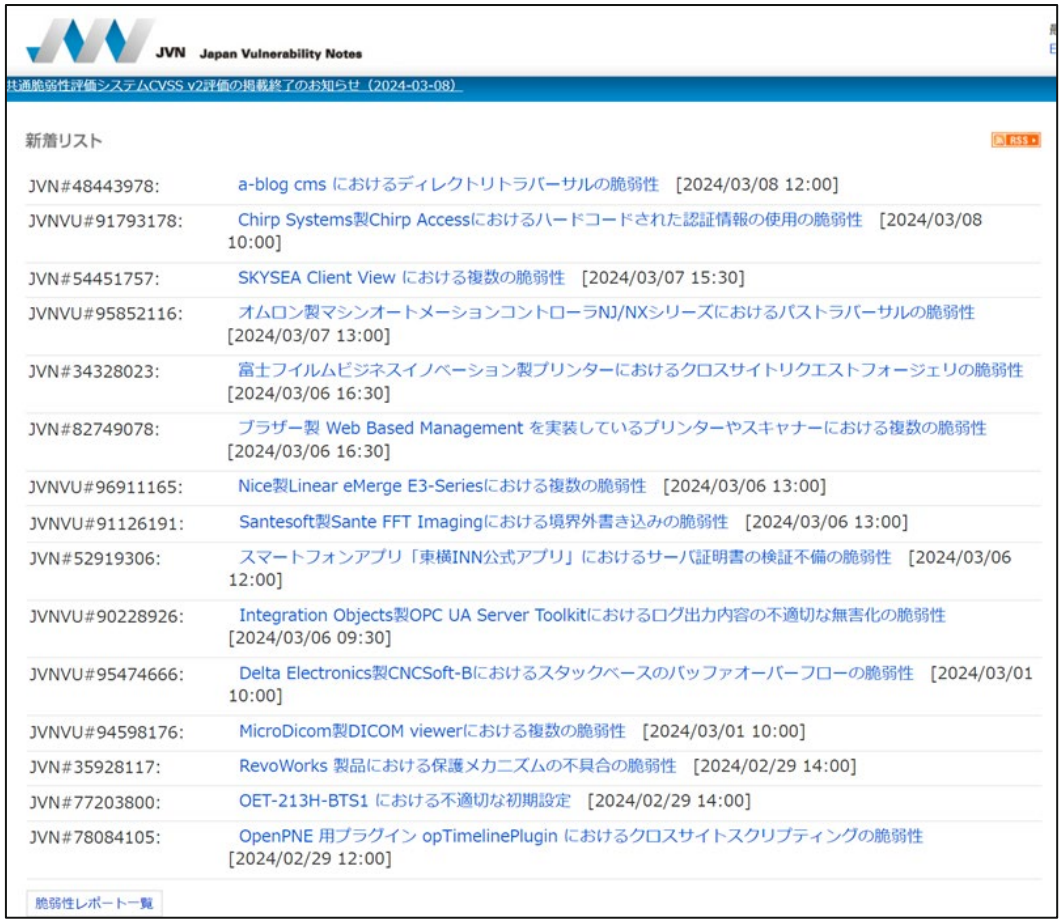
・サイバーセキュリティ注意喚起サービス「icat for JSON」

・**Twitter**「ICATalerts」　等

注意喚起サイト②

JVN (Japan Vulnerability Notes)

https://jvn.jp/



- JPCERT/CC、IPAが運営する「脆弱性対策情報ポータルサイト」
- 「情報セキュリティ早期警戒パートナーシップ」制度に基づいて報告され調整された脆弱性対策情報を掲載
- CERT/CC など海外の調整機関と連携した脆弱性対策情報を掲載

注意喚起サイト③

JPCERT/CC 注意喚起③

https://www.jpcert.or.jp/at/2024.html

Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起

最終更新: 2024-02-29

X ポスト　メール

JPCERT-AT-2024-0002
JPCERT/CC
2024-01-11（公開）
2024-02-29（更新）

I. 概要

2024年1月10日（現地時間）、IvantiはIvanti Connect Secure（旧: Pulse Connect Secure）およびIvanti Policy Secureゲートウェイにおける脆弱性に関するアドバイザリを公開しました。認証バイパスの脆弱性（CVE-2023-46805）とコマンドインジェクションの脆弱性（CVE-2024-21887）が対象で、脆弱性が組み合わされて悪用されると、遠隔の第三者が認証不要で任意のコマンドを実行する可能性があります。

Ivantiは本脆弱性を悪用する攻撃を確認しており、JPCERT/CCは本脆弱性を悪用したとみられる攻撃が国内組織に対しても行われた可能性があることを確認しています。また、1月16日に本脆弱性を実証するコード（Proof-of-Concept）が公開されて以降、本脆弱性を悪用するさまざまな攻撃が発生しています。本脆弱性の影響を受ける製品を利用している場合、後述「III. 対策」以降に記載の情報およびIvantiが提供する最新の情報を確認の上、回避策の適用や侵害有無を確認する調査などを推奨します。

- JPCERT/CCが公表する注意喚起情報
- 深刻且つ影響範囲の広い脆弱性などに関する情報を掲載
- 情報システムや制御システムに関わる端末やネットワークの構築・運用管理業務、組織内CSIRT業務、セキュリティ関連業務などに関与する担当者、技術者、研究者等が対象
- 官公庁系を含めて国内で広く参照されている

注意喚起サイト④

■ 警察庁：@police セキュリティポータル

https://www.npa.go.jp/bureau/cyber/koho/detect.html

Javaライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）を標的とした攻撃の観測について

2021年12月14日

概要

- Javaでログ出力に使われるライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）に関する情報が、The Apache Software Foundationから公表されています。
- 12月10日以降、当該脆弱性を標的とした攻撃を観測しています。

「Apache Log4j」の脆弱性に対する攻撃の観測状況（グラフ）

- 警察庁が公表する注意喚起情報
- 全国の警察施設のインターネット接続点に設置されたセンサーで観測したアクセス状況などを掲載
- 攻撃の事前準備として行われるサーバの稼働状況確認や脆弱性の有無の確認、脆弱性を悪用したコマンドの試行情報などを掲載

注意喚起サイト⑤

米国：CISA
(Cybersecurity and Infrastructure Security Agency)

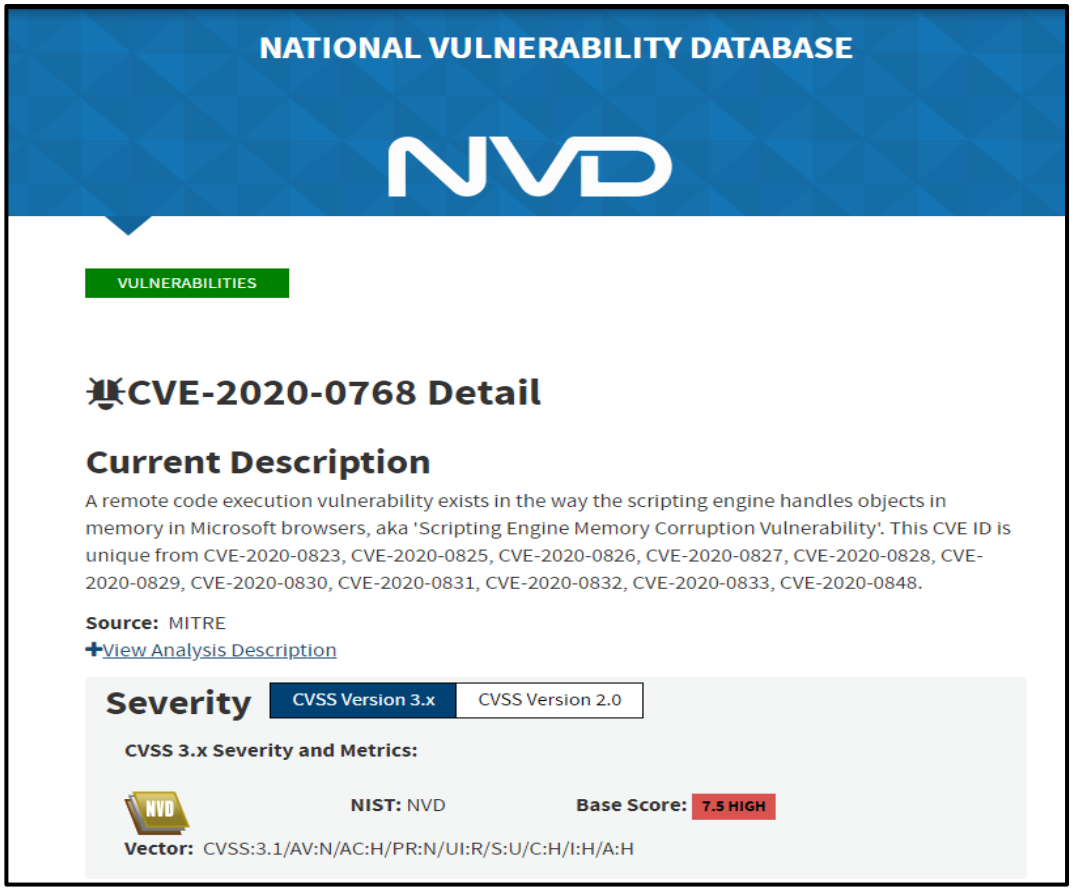
https://www.cisa.gov/

- アメリカの行政機関のひとつであり、米国土安全保障省の外局
- 制御システム向け勧告（ICS advisory）等を掲載
- 2023年２月24日にUS-CERTとICS-CERTが廃止となり、CISAに統合

脆弱性関連情報データベース①

NVD(National Vulnerability Database)

https://nvd.nist.gov/

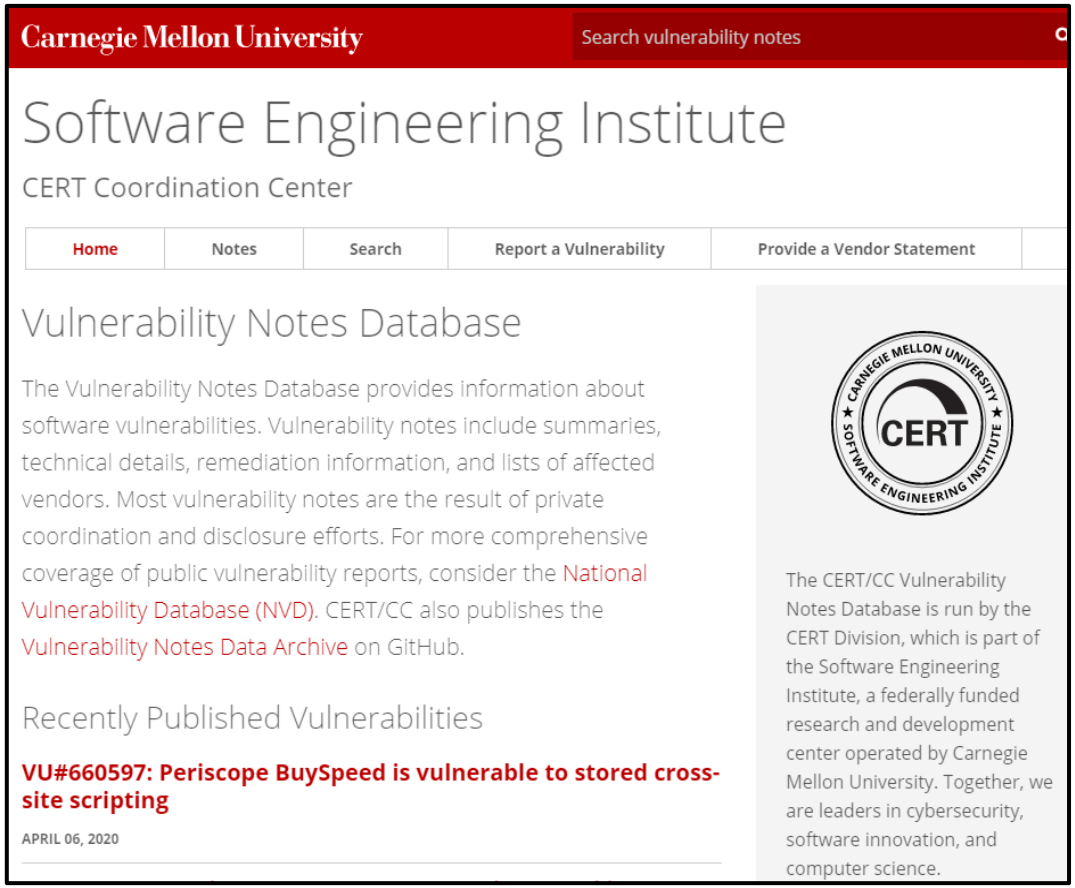


- 米国標準技術研究所（NIST）が運営
- CVEで管理されている
- DB検索機能、統計機能を備える
- 約22万件の脆弱性対策情報を登録（2024年2月時点）
- JVN iPediaの情報元の1つ

脆弱性関連情報データベース②

Vulnerability Notes Database

https://www.kb.cert.org/vuls/



- カーネギーメロン大学のソフトウェア工学研究所CERT/CCが運営
- CSIRTとして収集・発見した脆弱性情報を公開
- DB検索機能を備え、公開日やCVSS情報などで並び替えも可能
- 世界で初めてCERT/CCが設置された

製品ベンダーサイト①

定例アップデート提供

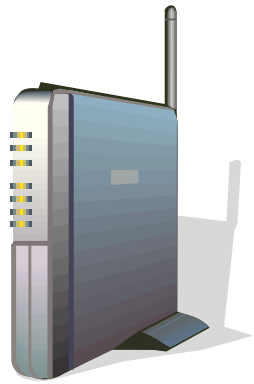
- マイクロソフト　（毎月第2火曜日 更新）
  https://msrc.microsoft.com/blog/categories/japan-security-team/
- オラクル　（年4回 1月,4月,7月,10月）
  https://www.oracle.com/security-alerts/

クライアント系

- アドビ　（Adobe Reader など）
  https://helpx.adobe.com/jp/security.html
- Mozilla　（Firefox/Thunderbird など）
  https://www.mozilla.org/en-US/security/advisories/
- Google(Google Chrome)
  https://chromereleases.googleblog.com/
- アップル
  https://support.apple.com/ja-jp/HT201222

製品ベンダーサイト②

- **サーバ、ネットワーク製品系**
  - シスコ　– セキュリティアドバイザリ
    https://tools.cisco.com/security/center/publicationListing.x
  - 日立 –セキュリティ情報
    http://www.hitachi.co.jp/hirt/security/index.html
  - IBM –Security Intelligence
    https://www.ibm.com/blogs/security/jp-ja/
  - Red Hat
    https://rhn.redhat.com/



製品ベンダーサイト③

オープンソース系

Apache Foundation

・Apache HTTP Server
https://httpd.apache.org/security/vulnerabilities_24.html

・Apache Tomcat
http://tomcat.apache.org/security.html

・Apache Struts
https://cwiki.apache.org/confluence/display/WW/Security+Bulletins

ISC （Internet Systems Consortium）

・BIND
https://kb.isc.org/docs/aa-00913

OpenSSL

https://www.openssl.org/news/vulnerabilities.html

WordPress

https://wordpress.org/news/category/security/

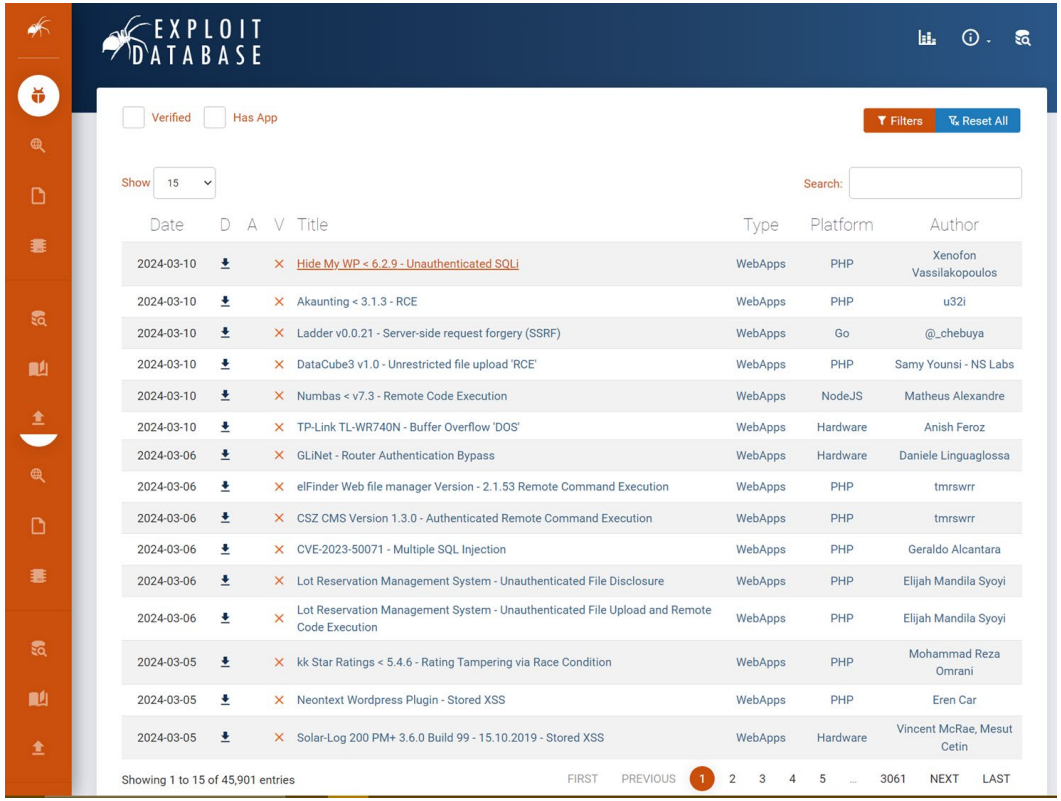
ニュースサイト

- **国内ニュースメディア**
  - ITmedia　エンタープライズ セキュリティ
    http://www.itmedia.co.jp/enterprise/subtop/security/index.html
  - 日経XTECH　セキュリティ
    https://tech.nikkeibp.co.jp/theme/security/
- 海外ニュースメディア
  - ComputerWorld Security　（米国中心）
    http://www.computerworld.com/category/security/
  - The Register Security　（英国・欧州中心）
    https://www.theregister.com/security/

攻撃情報①

Exploit Database

https://www.exploit-db.com/

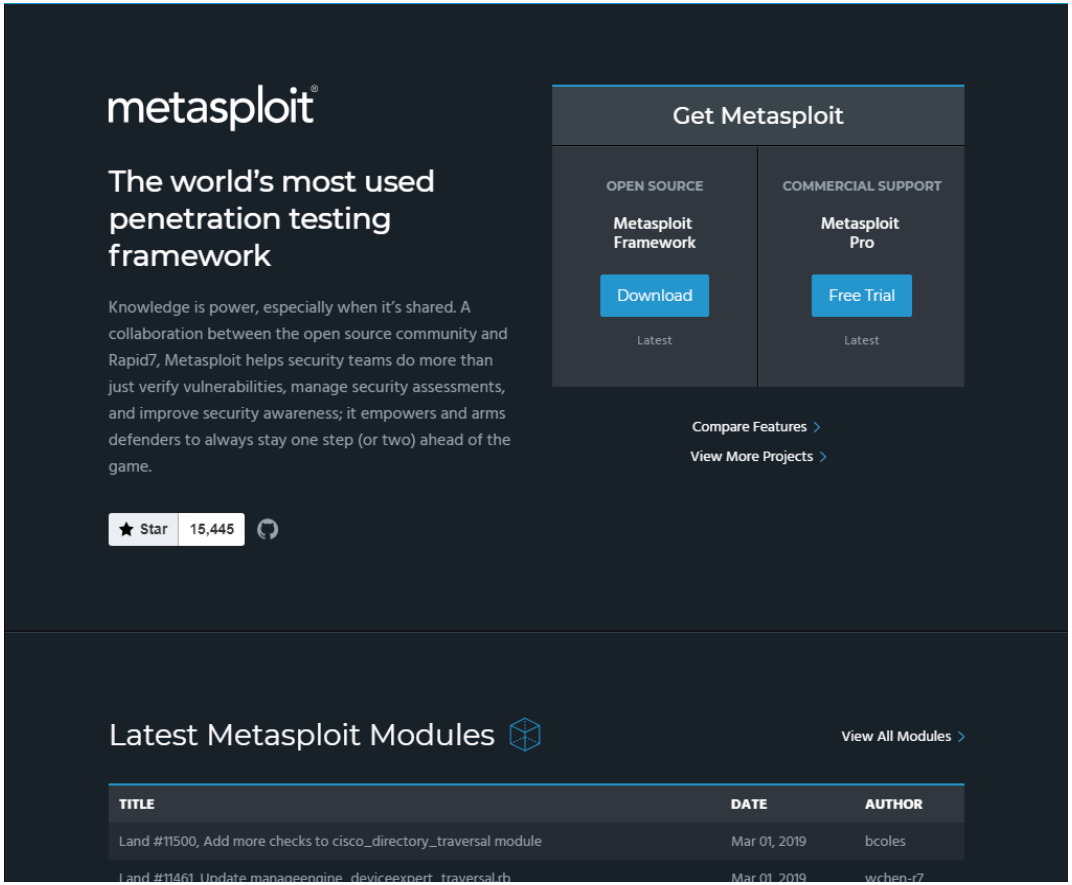


- Offensive Securityが運営する脆弱性の攻撃コード（exploit）の有無を確認できるデータベース
- ペネトレーションテスターや研究者向け

攻撃情報②

Metasploit

https://www.metasploit.com/

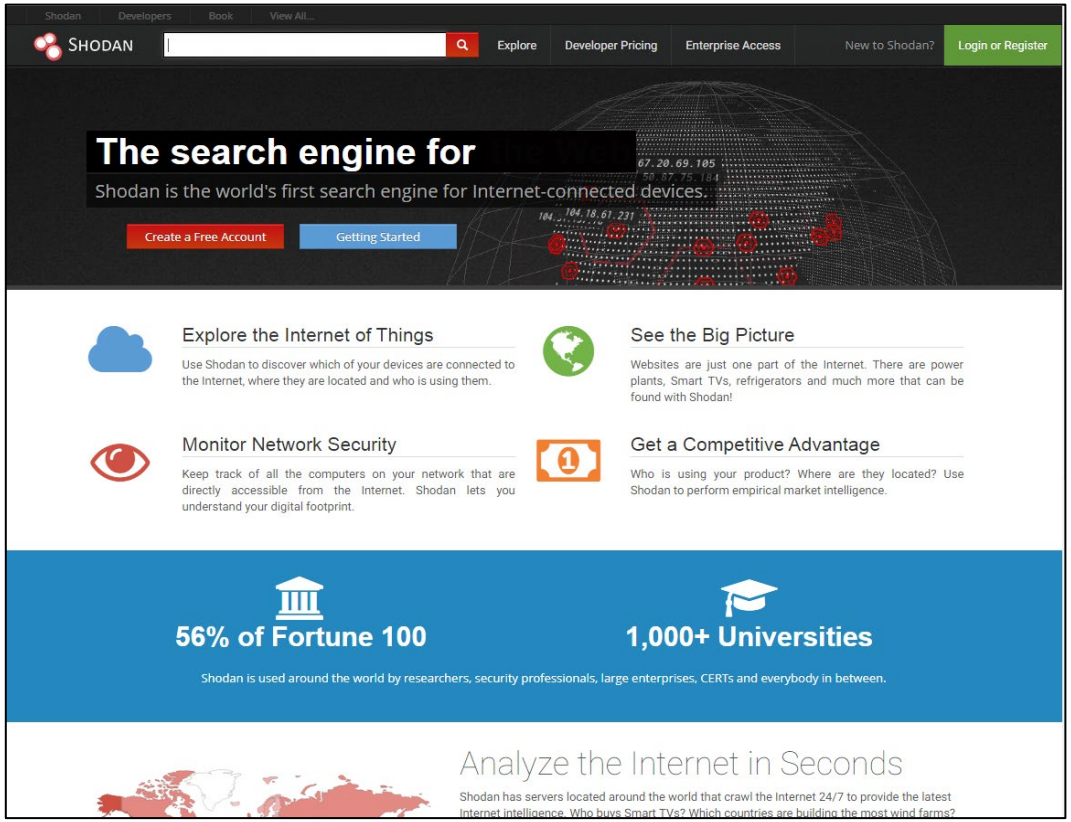


- Rapid7が運営する脆弱性の攻撃コード（exploits）をモジュールとして提供しているデータベース
- ペネトレーションテスターや研究者向け

脅威・動向に関する情報
意図せずインターネット上に晒されている機器があるかも？

SHODAN

https://www.shodan.io/



- インターネットにつながっている
  コンピュータ機器の検索エンジン
- サーバ、制御機器、オフィス機器など、
  5億台以上の情報を格納
- 認証が弱い機器や古いバージョンの
  まま運用している機器など、セキュリティ
  に問題がある機器も見つけることが
  可能
- 攻撃者は、攻撃の侵入口となり得る
  脆弱な機器を探すのに当サイトを
  使っていると言われている

最後に

脆弱性対策は日々の情報収集と
タイムリーな対策が重要です。
自組織にとって危険な脆弱性を
放置しないよう、
適切な対応を行いましょう。

セミナーに対する質問等について

本セミナーに対するアンケートの回答に
ご協力をお願いいたします。

「https://info.ipa.go.jp/form/pub/survey/isec-seminar」
受付期限：2023年3月31日までとなっております

本セミナーに関する質問等は
以下メールアドレスにご連絡ください。

「isec-labsemi-scap@ipa.go.jp」