

脆弱性対策情報収集ツール「MyJVN」を公開

～中小規模組織のセキュリティ対策のため、脆弱性対策情報の収集を効率化～

独立行政法人情報処理推進機構（略称：IPA、理事長：西垣 浩司）は、「JVN iPedia」（ジェイブイエヌ アイ・ペディア）の情報を、利用者が更に効率的に活用できるように、フィルタリング条件設定機能、自動再検索機能などを有した脆弱性対策情報収集ツール「MyJVN」（マイ・ジェイブイエヌ）を2008年10月23日（木）より公開しました。（URL: <http://jvndb.jvn.jp/apis/myjvn/>）

また、国際協力の強化に向けCPE（共通プラットフォーム一覧：Common Platform Enumeration）の試行を開始し、概説資料をIPAのウェブサイトで公開しました。

JVN iPedia¹は、日本国内向けの脆弱性対策情報データベースを目指し、国内で利用されているソフトウェア等の脆弱性の概要や対策情報を収集・蓄積しています。JVN iPedia は、現在 5,400 件を超える脆弱性対策情報を登録しています。

このたび、JVN iPedia に登録されたこれら多数の情報の中から、利用者が、利用者自身に関係する情報のみを効率的に収集できるように、フィルタリング条件設定機能、自動再検索機能、脆弱性対策チェックリスト機能などを有した脆弱性対策情報収集ツール「MyJVN」（マイ・ジェイブイエヌ）を開発しました。

また、MyJVN では、国際協力の強化に向け、米国政府の支援を受けた非営利団体の MITRE²が中心となって仕様策定を進めているソフトウェアの製品名を記述するための共通の基準である CPE（共通プラットフォーム一覧：Common Platform Enumeration）の試行を開始しました。

すでに、JVN iPedia、MyJVN では、CVE³、CVSS⁴、CWE⁵を適用しています。今回の CPE 適用に引き続き、今後も共通基準の導入を進めることにより、利用者側の客観的・効率的な脆弱性対策を目指した利活用基盤を整備していきます。

1. 利用者に関する脆弱性対策情報のみを提示

(1) フィルタリング条件設定機能

MyJVN は、JVN iPedia に登録されている脆弱性対策情報のうち、利用者に関する情報のみを表示することができます。利用者が使用しているソフトウェアのベンダ名（図 1）と製品名（図 2）を選択すると、関連する脆弱性対策情報のみを表示します（図 3）。

さらに、脆弱性対策情報一覧の中から一つをクリックすると詳細な脆弱性対策情報を見ることができます（図 4）。「脆弱性対策情報 詳細情報」画面では、影響を受けるシステムや影響を受けた時の深刻度、対策情報などが表示されます。

¹ IPA が公開している脆弱性対策情報データベース。<http://jvndb.jvn.jp/>

² MITRE Corporation。米国政府向けの技術支援や研究開発を行う非営利組織。<http://www.mitre.org/>

³ CVE: Common Vulnerabilities and Exposures。<http://cve.mitre.org/index.html>

⁴ CVSS: Common Vulnerability Scoring System。「共通脆弱性評価システム CVSS v2 概説」を参照下さい。
<http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html>

⁵ CWE: Common Weakness Enumeration。「共通脆弱性タイプ一覧 CWE 概説」を参照下さい。
<http://www.ipa.go.jp/security/vuln/CWE.html>

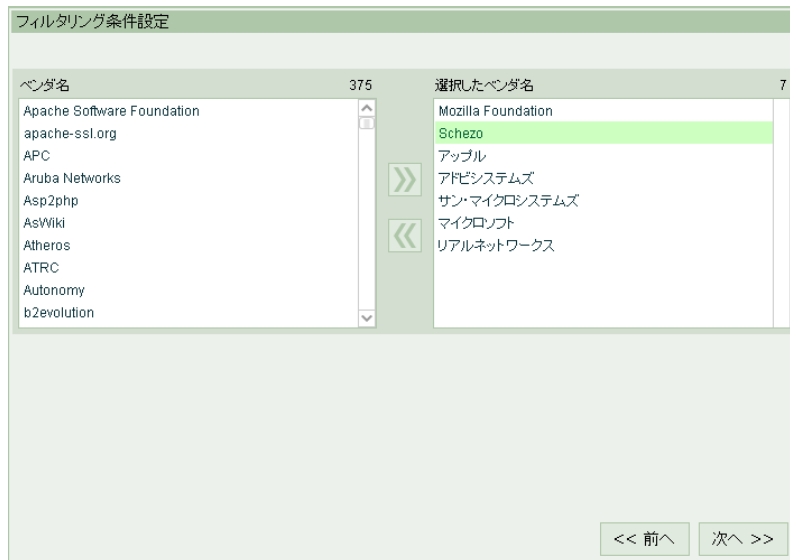


図 1. ベンダ名選択画面

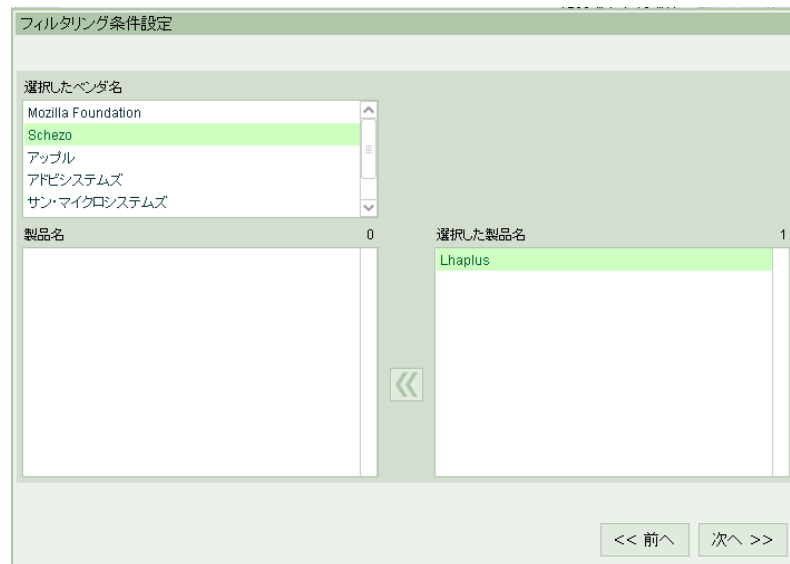


図 2. 製品名選択画面

⊕	JVNDB-2008-001744	2008.10.16 13:39:48	Linux Kernel の do_change_type 関数における権限昇格の脆弱性
⊕	JVNDB-2008-001743	2008.10.16 13:39:35	Linux Kernel の vfs 実装におけるサービス運用妨害 (DoS) の脆弱性
⊕	JVNDB-2008-001742	2008.10.16 13:39:18	Linux Kernel の dio サブシステムにおけるサービス運用妨害 (DoS) の脆弱性
⊕	JVNDB-2008-001741	2008.10.16 13:39:02	Linux Kernel の sound サブシステムにおける重要な情報が漏えいする脆弱性
⊕	JVNDB-2008-001740	2008.10.16 13:38:37	Windows 上の ISC BIND におけるサービス運用妨害状態 (DoS) の脆弱性
⊕	JVNDB-2008-001739	2008.10.15 15:27:00	Apple Mac OS X 上で起動している Java の file:// URL アクセスにおける任意のプログ...
⊕	JVNDB-2008-001738	2008.10.15 15:26:34	Apple Mac OS X 上で起動している Java の HMC プロバイダにおける任意のコードを...
⊕	JVNDB-2008-001736	2008.10.15 15:26:06	Sun Solaris の Solaris Access Control List (ACL) 処理における NULL ポインタ参照...
⊕	JVNDB-2008-001735	2008.10.15 15:25:45	Sun Solaris におけるタグの取り扱いに関する権限昇格の脆弱性
⊕	JVNDB-2008-001160	2008.10.15 15:23:30	Sun JDK/JRE の色彩処理ライブラリにおけるサービス運用妨害 (DoS) の脆弱性
⊕	JVNDB-2008-001161	2008.10.15 15:23:10	Sun JDK/JRE の画像処理ライブラリにおける権限昇格の脆弱性
⊕	JVNDB-2008-001524	2008.10.15 15:22:49	Sun JDK/JRE の JMX 管理エージェントにおける認証なしの操作を実行される脆弱性
⊕	JVNDB-2008-001533	2008.10.15 15:22:36	Sun Java Web Start における任意のファイル作成される脆弱性
⊕	JVNDB-2008-001534	2008.10.15 15:22:20	Sun Java Web Start における任意のファイルを作成/削除される脆弱性
⊕	JVNDB-2008-001535	2008.10.15 15:22:05	Sun Java Web Start における情報漏えいの脆弱性
⊕	JVNDB-2008-001536	2008.10.15 15:21:52	Sun JDK/JRE の Secure Static Versioning における古い JRE のアップデートの実行処...
⊕	JVNDB-2008-001734	2008.10.14 15:09:58	PHP の memnstr 関数におけるバッファオーバーフローの脆弱性
⊕	JVNDB-2008-001733	2008.10.14 15:09:47	PHP の imageloadfont 関数におけるバッファオーバーフローの脆弱性
⊖	JVNDB-2008-001158	2008.10.14 15:08:11	Sun JDK/JRE の Java Web Start におけるスタックベースのバッファオーバーフローの...

図 3. フィルタリングした脆弱性対策情報一覧画面



図 4. 脆弱性対策情報 詳細情報

(2) 自動再検索機能

一度フィルタリング条件を設定しておけば、2 回目以降はアクセスするだけで同じ条件で検索を行いますので、(1)のベンダ名選択 (図 1) や製品名選択 (図 2) を再度設定する必要がありません。利用者は MyJVN の画面を開くだけで、常に自分に関係する最新の脆弱性対策情報を確認することができます。

(3) 脆弱性対策チェックリスト機能

脆弱性対策が具体的にどこまでできているか確認するためには、脆弱性対策チェックリスト機能を使います。脆弱性対策チェックリスト機能には、脆弱性対策情報の発行日、脆弱性 ID とそのタイトル、脆弱性の概要、深刻度、影響を受けるシステムなどが表示されますので、脆弱性の対応状況を把握する際には、プリントアウトすることで脆弱性対策のチェックリストとして利用することができます (図 5)。

脆弱性対策チェックリスト						
No	発行日	ID/タイトル	概要	深刻度	影響を受けるシステム	更新日
1	2008.07.09	JVND-2008-001744 Linux Kernel の do_change_type 関数における権限昇格の脆弱性	Linux Kernel の fs/namespace.o における do_change_type 関数には、CAP_SYS_ADMIN ケーパビリティを持つ発信元を確認しないため、権限昇格およびサービス運用妨害状態 (DoS) の脆弱性が存在します。	中	linux - linux_kernel redhat - enterprise_linux - enterprise_linux_desktop	2008.10.16
2	2008.08.12	JVND-2008-001743 Linux Kernel の vfs 実装におけるサービス運用妨害 (DoS) の脆弱性	Linux Kernel の vfs 実装における fs/namei.o の real_lookup 関数および __lookup_hash 関数には、削除されたディレクトリに対する子 dentry の作成を防止しないため、サービス運用妨害状態 (DoS) の脆弱性が存在します。	中	linux - linux_kernel redhat - enterprise_linux - enterprise_linux_desktop	2008.10.16
3	2008.09.04	JVND-2008-001742 Linux Kernel の dio サブシステムにおけるサービス運用妨害 (DoS) の脆弱性	Linux Kernel の dio サブシステムにおける fs/directio.o には、dio 構造物を適切に初期化しない不備が存在するため、サービス運用妨害状態 (DoS) となる脆弱性が存在します。	中	linux - linux_kernel redhat - enterprise_linux - enterprise_linux_desktop	2008.10.16
4	2008.08.08	JVND-2008-001741 Linux Kernel の sound サブシステムにおける重要な情報が漏えいする脆弱性	Linux Kernel の sound サブシステムにおける sound/core/seq/oss/seq_oss_synth.o の snd_seq_oss_synth_make_info 関数には、送信元に特定のデータを返す前に max_synthdev によって定義された範囲のデバイス番号にあることを確認しないため、重要な情報が漏えいする脆弱性が存在します。	中	linux - linux_kernel redhat - enterprise_linux - enterprise_linux_desktop	2008.10.16
5	2008.09.22	JVND-2008-001740 Windows 上の ISC BIND におけるサービス運用妨害状態 (DoS) の脆弱性	Windows 上の ISC BIND には、UDP パケットの処理に不備があり、サービス運用妨害状態 (DoS) にされる脆弱性が存在します。	高	iso - bind	2008.10.16
6	2008.09.24	JVND-2008-001739 Apple Mac OS X 上で起動している Java の file:// URL アクセスにおける任意のプログラムを実行される脆弱性	Apple Mac OS X 上で起動している Java には、file:// URL にアクセスすることを防止しないため、任意のプログラムを実行される脆弱性が存在します。	高	apple - mac_os_x - mac_os_x_server	2008.10.15
7	2008.09.24	JVND-2008-001738 Apple Mac OS X 上で起動している Java の Hash-based Message Authentication Code (HMAC) プ	Apple Mac OS X 上で起動している Java の Hash-based Message Authentication Code (HMAC) プ	高	apple - mac_os_x	2008.10.15

図 5. チェックリスト画面

2. CPE の試行運用を開始

CPE（共通プラットフォーム一覧：Common Platform Enumeration）は、情報システムを構成する、ハードウェア、ソフトウェアなどを識別するための共通の名称基準です。米国政府の支援を受けた非営利団体の MITRE が中心となって仕様策定を進めており、2007 年 1 月 30 日に原案である CPE バージョン 1.0 が公開されました。

その後、米国の脆弱性対策データベースである NIST⁶の NVD⁷、米国政府のデスクトップ基準である FDCC⁸（Federal Desktop Core Configuration）での適用を通して、仕様改善が行われ、2008 年 1 月 31 日に CPE バージョン 2.1 が公開されました。

MyJVN には、NVD が公開している CPE Dictionary を参考に、JVN iPedia で公開するそれぞれの脆弱性対策情報を CPE 名で関連付ける機能があります。

今後、NIST が提供する CPE Dictionary との連携や、製品識別子としての CPE 名を利用することで、脆弱性対策情報の提供および流通基盤の整備を図るなど、検討を行っていきます。

CPE に関しては次の URL の「共通プラットフォーム一覧 CPE 概説」を参照下さい。

<http://www.ipa.go.jp/security/vuln/CPE.html>

■ 本件に関するお問い合わせ先

独立行政法人 情報処理推進機構 セキュリティセンター 小林／杉山
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp

■ 報道関係からのお問い合わせ先

独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

⁶ NIST: National Institute of Standards and Technology。米国国立標準技術研究所。米国の科学技術分野における計測と標準に関する研究を行う機関。<http://www.nist.gov/>

⁷ NVD: National Vulnerability Database。NIST が運営する脆弱性データベース。<http://nvd.nist.gov/>

⁸ FDCC: Federal Desktop Core Configuration。米国政府が各省庁に向けて、デスクトップ環境の最低限のセキュリティ設定を実施するように定めた基準。<http://nvd.nist.gov/fdcc/index.cfm>