Press Release

2024 年 11 月19 日
フューチャー株式会社
(東証プライム:証券コード 4722)

脆弱性管理ソリューション「FutureVuls」追加機能をリリース
外部スキャンツールとの機能連携、ランサムウェア攻撃への対応強化など大幅アップデート

フューチャー株式会社(本社:東京都品川区、代表取締役会長兼社長 グループ CEO 金丸恭文、以下フューチャー)は、エンタープライズ向けに独自開発した脆弱性管理ソリューション「FutureVuls」※1に統合的な社内外の脆弱性管理に向けた新機能を追加し、2024 年 10 月 21 日にリリースしました。

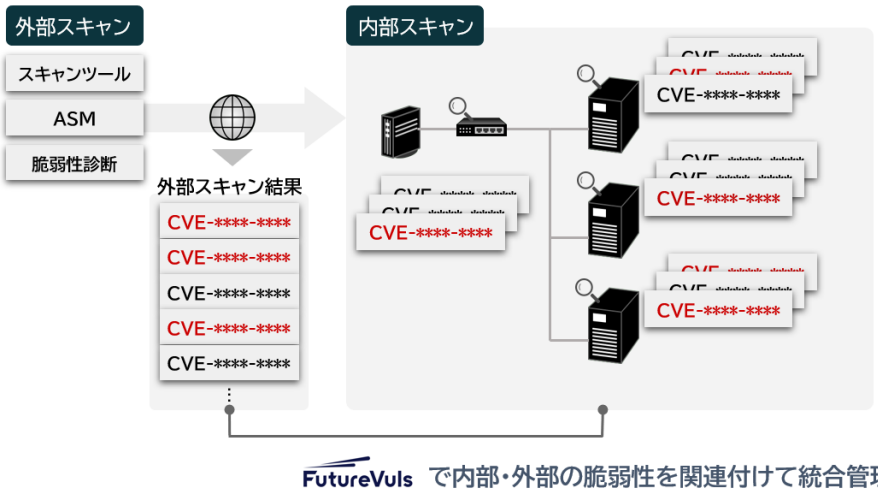
「FutureVuls」は、システムの脆弱性検知から情報収集、対応判断、タスク管理、パッチ適用といった脆弱性管理の一元化と徹底的な自動化を可能にしたソリューションです。脆弱性情報は年間数万件※2 が新たに公開されていますが、FutureVuls は管理下のシステムに関係する脆弱性のみを検出し、対応判断に必要な情報をまとめて表示するなど、システム内の脆弱性を可視化します。予防的な観点からサイバーセキュリティ対策を重要視する多くの企業に採用され、脆弱性管理の自動化による工数削減と効率的な運用に効果を発揮しています。

2022 年 9 月には脆弱性評価のフレームワーク SSVC をベースとした自動トリアージエンジンを搭載※3し、2023 年 2 月には OSS として Windows 用スキャナを公開※4するなど、フューチャーでは時代の要請にこたえて様々な FutureVuls の機能追加を行ってきました。今回のアップデートでは、①外部スキャンツールの結果インポート機能、②SSVC 自動トリアージにおける脅威情報の取り込み範囲拡大および警戒すべき情報の表示機能を追加するほか、③SSVC の決定木を最新版に更新しました。

【追加機能】

1　外部スキャンツールの結果インポート機能

Nessus や OpenVAS、Nmap などのスキャンツール※5 に加え、ASM(Attack Surface Management)ツール、Web 脆弱性診断、PCI-DSS(Payment Card Industry Data Security Standard)の脆弱性スキャン結果などが FutureVuls に取り込めるようになり、外部からのインターネット攻撃に対する脆弱性と内部脆弱性の一元管理が可能になります。



FutureVuls で内部・外部の脆弱性を関連付けて統合管理

2　ランサムウェアによる攻撃情報を含めた脅威情報の取り込み強化

これまで脆弱性判断における重要なリソースとして活用してきた KEV カタログ(Known Exploited Vulnerabilities Catalog)※6 において、ランサムキャンペーンで利用される特定の脆弱性を示す情報が追

加公開※7されたことを受けて、FutureVuls での対応判断への活用と表示強化を開始しました。管理下にあるシステムのどのサーバにランサムキャンペーンで利用されている脆弱性が含まれているかを明確にし、ランサムウェア対策への優先的な対応をサポートします。

3　**SSVC 決定木を最新版のバージョン 2.1 に更新**

この更新によって手動で設定が必要な項目が減り、利用時の設定が容易になります。

フューチャーは、今後も最新の脆弱性情報を活用し、FutureVuls をはじめとした最先端のソリューションの開発、改善を続けていくとともに、IT・OT・IoT 全ての領域を支援する総合的なセキュリティコンサルティングサービスを提供することで、あらゆる業種・業界のお客様の未来に新たな価値を創造します。

※1. FutureVuls 製品サイト：https://vuls.biz/lp/
※2. 共通脆弱性識別子「CVE」（Common Vulnerabilities and Exposures）を特定、管理する Web サイト「cve.mitre.org」に公開される脆弱性情報の件数。
※3. プレスリリース「継続的脆弱性管理サービス「FutureVuls」に最新の評価手法「SSVC」を導入～リスクベースの「対応判断」から「対応指示」までを全自動化」：https://www.future.co.jp/press_room/PDF/PressReleasea_FutureVuls_SSVC_20220914.pdf
※4. プレスリリース「継続的脆弱性管理サービス「FutureVuls」 Windows のための脆弱性スキャナを OSS 化」：
https://www.future.co.jp/press_room/PDF/PressRelease_FutureVuls_OSS_230217.pdf
※5. 本プレスリリースに記載する製品名（Nessus、OpenVAS、Nmap）は各社の商標または登録商標です。
※6. 米国の行政機関 CISA(Cybersecurity & Infrastructure Security Agency)が「実際に悪用された脆弱性の信頼できる情報源」として公開するカタログ（Known Exploited Vulnerabilities Catalog）：https://www.cisa.gov/known-exploited-vulnerabilities-catalog
FutureVuls では 2021 年 12 月より CISA-KEV カタログのデータを取り込み、SSVC 自動トリアージにおける脅威情報として利用しています。（https://help.vuls.biz/release-note/20211209/）
※7. CISA は 2023 年 10 月より KEV カタログデータにランサムキャンペーンで利用されている脆弱性を示すフィールドを追加：https://www.cisa.gov/news-events/alerts/2023/10/12/cisa-releases-new-resources-identifying-known-exploited-vulnerabilities-and-misconfigurations-linked

■FutureVuls に関するお問い合わせ先
https://vuls.biz/lp/contact

■本件に関する報道機関からのお問合せ先
フューチャー株式会社　広報担当：松本、石井　　TEL：03-5740-5721
お問い合わせフォーム：https://www.future.co.jp/apps/contact/corp/press_interview_entry.php