



2014年11月20日

報道関係者各位
No. 63103

テナブル ネットワーク セキュリティ ジャパン 株式会社
株式会社東陽テクニカ

**Tenable Network Security が Nessus v6 をリリース、
標的型攻撃のリスクを減らすために高度なシステムハードニング、
マルウェア検知、モバイル対応を強化**

**パワフルな脆弱性管理プラットフォームが、アクティブスキャン機能を自動化、簡素化し、
サイバーセキュリティの死角をなくすための機能を拡張**

※ 本資料は、米国で 2014 年 11 月 18 日（現地時間）に発表されたプレスリリースの日本語訳です。

ネットワークの継続的モニタリングにおけるリーダーである米国 Tenable Network Security®社は、11 月 18 日、高度なマルウェア検出、ポリシー設定とコンプライアンス、モバイル、仮想環境、クラウド対応を通じて、ユーザのセキュリティリスクを減らす、Nessus® の v6 のリリースを発表しました。

多くの検出と修復のストラテジーが有効に働かないことがあります、これは適切なシステム設定がなされていないためで、ベストプラクティスの実装が欠如していた結果とも言えます。Tenable では、Nessus v6 にスキャン設定のための 12 種類のテンプレート、100 以上のシステム強化のガイドラインを用意し、ユーザは脆弱性とマルウェアの検知を容易に実行し、推測や勘に頼ったセキュリティとコンプライアンスの持続的な設定に時間をかける必要がなくなります。

「Nessus v6 は、IT インフラ全体のシステムポリシーの強化と、脆弱性、コンフィグレーション、パッチ管理の統合的なアプローチを提供することにより、ユーザの攻撃面を保護します」と Tenable Network Security の CEO である Ron Gula（ロン・グーラ）は述べています。

「これは、モバイル機器、BYOD、仮想システムとクラウドアプリケーションを含めた全てのネットワークリソースへのリスクを減らすことを意味し、セキュリティチームにはあらゆるネットワークの脆弱性が通知されます。」

Nessus v6 は、現在最も急速に攻撃対象セグメントの 1 つとなっているモバイルデバイスをサポートします。代表的なエンタープライズモビリティ管理 (EMM) ソリューションと統合することにより Nessus v6 は、ネットワークに接続する全ての認証済みデバイスをスキャンし、認証されていないデバイスは検知され、セキュリティ管理者が適切な対処を行えることとなります。

Nessus v6 は、アクティブスキャンを簡素化、自動化し拡張することで、あらゆる分野のユーザのサイバーディフェンス強化をサポートします。より巧妙化するマルウェアへの対策として、Nessus v6 では不正侵入に対し、エンドポイントの直接スキャンにより既知のマルウェアを、ネットワークの状態を監視することで、より高度化された未知の脅威を見つけることが可能です。

「エンタープライズ企業の多くが、既知の脆弱性と未知の脆弱性のいずれも利用した、最も侵入しやすいルートからの巧妙な攻撃と脅威に日々対応せざるを得ない、と感じている」と Tenable Network Security の最高製品責任者 (CPO)、ルノー・デレイソンは述べています。

「Nessus v6 は、そのようなユーザから、コントロールを取り戻せるように開発されています。新しいマルウェア対策、システムハードニングのテンプレートおよびモバイルのサポートと Tenable の高品質なスキャン機能の組み合わせは、最新の脆弱性、脅威やリスクを検知、識別を強力にサポートし、組織全体をより有効に防衛することを可能とします。」

Nessus v6 に追加された新機能には、社内コンプライアンス基準に容易に編集できるスキャンポリシーエディタ、スキャン履歴を管理するヒストリー・タブ、および、より広範の IT 環境へ Nessus v6 を統合させる RESTful API が含まれます。

以上

Nessus v6 についての情報は以下にて確認いただけます (いずれも英文サイト)。

- [What's New in Nessus v6?](#)
- [Nessus v6 FAQ](#)
- [Reducing Your Attack Surface webcast](#)
- [Nessus Discussion Forum](#)

Tenable Network Securityについて

テナブル ネットワーク セキュリティは、近年、年々進化する新たな外的脅威、ネットワーク上の脆弱性、コンプライアンスに関連するリスクから自社を守るセキュリティ製品として、米国防総省をはじめ、20,000 を超える政府機関、大手企業などに利用されています。同社の Nessus® および SecurityCenter™ 製品は、脆弱性の検出、サイバー攻撃防止、また様々な規制要求へのコンプライアンス遵守に対応するためのツールとして、業界を代表する製品として広く認知されています。なお、テナブル ネットワーク セキュリティでは、東陽テクニカとの契約締結に先立ち、2013 年 11 月に日本法人、Tenable Network Security Japan 株式会社を設立しています。テナブル ネットワーク セキュリティに関する詳細は、www.tenable.com をご覧ください。

東陽テクニカについて

東陽テクニカは昭和 28 年の設立より「技術と情報」をキーワードに、最先端の「測るツール」を主として欧米の電子計測器メーカーより輸入し、日本の技術発展に寄与することを使命として、日本の研究者・開発者に提供してきました。「電子技術センター」における修理、校正、技術サポートや自社製品の開発、「テクノロジーインターフェースセンター」で行うお客様向けの各種セミナー・トレーニングなどの取組みは、400 人を超える全従業員の 8 割を占めるエンジニアの技術力に裏付けられています。東陽テクニカはこれからも、「テクノロジーインターフェース」の使命を果たすべく努力してまいります。東陽テクニカに関する詳細はwww.toyo.co.jp をご覧ください。

【お問い合わせ先】

株式会社トレイントラックス（テナブル ネットワーク セキュリティ 広報代理店）

担当： 小牧、原田

TEL： 03-5738-4177

MAIL： pr@traintracks.jp

株式会社東陽テクニカ（テナブル ネットワーク セキュリティ 販売代理店）

情報通信システム営業部

担当： 高垣 景二

TEL： 03-3245-1250

MAIL： tenable@toyo.co.jp