報道関係各位

2018 年 1 月 31 日
タニウム合同会社

数百万台のエンドポイントを数秒で可視化
エンドポイントプラットフォームを提供する「タニウム合同会社」
CPU の脆弱性「Meltdown」「Spectre」、タニウム社の対応を紹介

数百万台のエンドポイントを 15 秒で可視化できるプラットフォームを提供する『タニウム合同会社』(以下:タニウム社日本法人、所在地:東京都千代田区、代表執行役社長:古市力)は、CPU の脆弱性「Meltdown(メルトダウン)」「Spectre(スペクター)」のタニウム社の対応についてお知らせします。

「メルトダウン」「スペクター」の影響を受けるマイクロプロセッサは全世界の全コンピュータ内にあると言っても過言ではなく、デスクトップやサーバーのみならず、クラウドインフラにまで影響を及ぼす可能性があります。IT 部門にとっては、アセットの特定から修正の実施、その後のモニタリングを幾度となく繰り返す必要があるため、まさにそれらとの戦いと感じられるでしょう。

また「メルトダウン」「スペクター」は複合的なハードウェアの脆弱性からなり、単体のパッチを適応することで修正できるものではありません。これらの解決のためには、「アセットの識別と整理」「互換性テスト」「影響を受けるハードウェア、OS、アプリケーションへのパッチ適応」「システムパフォーマンスのモニタリング」と言った複数フェーズに渡り、IT オペレーションとセキュリティのチームが協力して対応する必要があります。

今回、タニウム社が提供可能な解決策として、「可視化」「パッチ適応」「パフォーマンスのモニタリング」そして「検出と対応」の手法について解説します。

＜可視化＞

今回の脆弱性を踏まえた上で、まずは環境の全体像を把握するために、影響を受けたハードウェアの完全なリストを作成する必要があります。

Tanium Platform では、検索画面に「Get CPU Details from all machines」と入力するだけで、管理下端末すべての CPU 製造メーカーやプロセッサ詳細などのハードウェア情報を可視化することができます。この機能を使用することにより、「メルトダウン」「スペクター」の影響を受ける可能性があるハードウェアの特定も可能です。Tanium のアセットはこのコンテンツをさらに追求し、ハードウェア、OS、ソフトウェア、パッチ、ユーザーデータを含む幾多のエンドポイント属性を集約した上で、正確かつ完全な総括レポートを生成することが出来ます。

このデータが必要となるのは単純に CPU 関連のみならず、ウェブブラウザといったようなサードパーティのアプリケーションも「スペクター」の影響下にあるために該当し、将来的にはアップデートが必須となります。そのため、広範囲にわたる問題であり、環境内にてインストールされた脆弱性に影響し得るソフトウェアの数ヶ月単位での透明性を確実に維持し、制御する必要があります。

＜パッチ適応＞

「メルトダウン」に対応する上で、OEM ベンダーによって提供される幾多のハードウェアパッチや、それを適用させるために複数の OS を操作する必要が発生します。ベンダーからの最新情報やアップデートは随時更新されていますが、いかなるパッチ適応においても同様で、一定以上の該当機材がある場合に迅速な作業を実施し、インストールを確認、予期せぬ事態に対応することは困難です。

Tanium のアーキテクチャは、数百数千から構成されるシステムであろうと、1台の Tanium サーバーを用いて効率よくパッチとサポートファイルを配布し、インストールを可能にします。Tanium Patch は、これにスケジューリング、ブラックリスト、カスタムワークフローなど、Windows 用パッチのマネジメントと展開を容易にする機能を付加しています。さらに、Tanium の追加コンテンツを使用することによって、Linux、OS X、Solaris、そして AIX プラットフォームに、パッチやその他カスタムパッケージを展開することが出来ます。

また、Microsoft 社がアンチウィルスソフトによっては互換性の問題からブルースクリーンや他エラーが発生する可能性がある、と発表したことがさらに今回の問題を複雑にしています。Microsoft 社によると、自動アップデートによってシステムを不安定にするリスクを低減するため、パッチが有効になるようにアンチウィルスソフトウェアによる指定のレジストリ値（例：互換性アップデート中の hotfix）を個別設定することを必須としています。
このようなイレギュラーな対応が必要となっても、Tanium のお客様は、「Registry Key Value Exists」などのセンサーを使用し、どのシステムが上記の指定レジストリ値を欠いているかを数秒のうちに把握することが出来ます。さらに、提供済みの Installed Applications センサーや他のセンサーと併用することで、アンチウィルスのアップデート状況を追跡し、必要なレジストリ変更を承認することが可能となります。

＜パフォーマンスモニタリング＞

これらパッチの適用による変更は一定のワークロードにおいて、プロセッサのパフォーマンスに悪影響を及ぼす可能性があります。実際のワークロードのオーバーヘッド値は使用しているソフトウェアやハードウェアによって変動するわけですが、パフォーマンス必須であるシステム、バーチャルマシンを稼動させている拡張されたハードウェア、もしくは正確な割り当てが必要なクラウドのホストを運用する組織にとって、これは大きな弊害となります。

Tanium は、各プロセスおよびアプリケーションの使用する CPU 稼動値を含め、Windows、Linux、OS X、そして UNIX 上にて詳細なパフォーマンス値を取得する機能を提供しています。このデータの傾向をトレースすることによって、時間経過を軸とした継続的なパフォーマンス報告を含め、いかなるエンドポイントのデータセットや数値も可視化できます。たとえば、パッチを展開する前に実施することにより、影響を受けているシステム上の現時点でのリソース使用を各グループ毎での基準値を見積もることが可能となります。また、パッチを展開後に実施することによって、プロセッサ動作の変化の度合いを確認し、悪影響を及ぼしているパフォーマンス変動や変更が必要となるシステムの特定に役立ちます。

＜検出と対応＞

研究者によると、「スペクター」と「メルトダウン」の脆弱性を利用する手法は通常のアプリケーションによる行動から判別するのが難しいと言われています。つまり、通常使用しているEDRやアンチマルウェアといったツールでの検出には期待できません。しかし、これらの脆弱性を利用するにあたり、攻撃者は標的としたエンドポイントにて悪質なコードを実行する権限を取得する必要があります。この条件を踏まえ、侵入後の「スペクター」および「メルトダウン」を活用したペイロードが実行される前に攻撃を阻止するための対策を継続することが重要です。

Tanium Threat Responseは、MITREのATT&CK Frameworkによってカテゴリー化された攻撃手法も含めて、悪質な活動を検出して捜査する総合的なソリューションを提供しています。Taniumの Endpoint Detection and Responseはリアルタイムでアラートを出すための定期的な更新フィードと、異常値を特定するためのワークフローをお客様に提供しています。

【タニウム社について】

タニウム社は2007年に発足し、5年間の製品開発を経て2012年末にタニウムプラットフォームの販売をアメリカで開始、日本には2015年10月に本格参入しました。秒単位で数十万台のエンドポイントを保護、制御、管理する独自の価値を提供するタニウムの製品は、IT部門の担当者に幅広く受け入れ、金融庁が定めるG-SIBS(グローバルなシステム上重要な銀行及び国内のシステム上重要な銀行)30行のうち16行に導入されております。

アメリカでは、銀行の上位15社のうち12社、小売業の上位10社のうち6社が含まれています。