Ivanti Neurons Patch for MEM (Microsoft Endpoint Manager)

リスクに基づくサードパーティーパッチパブリッシングでMicrosoft Intuneを拡張

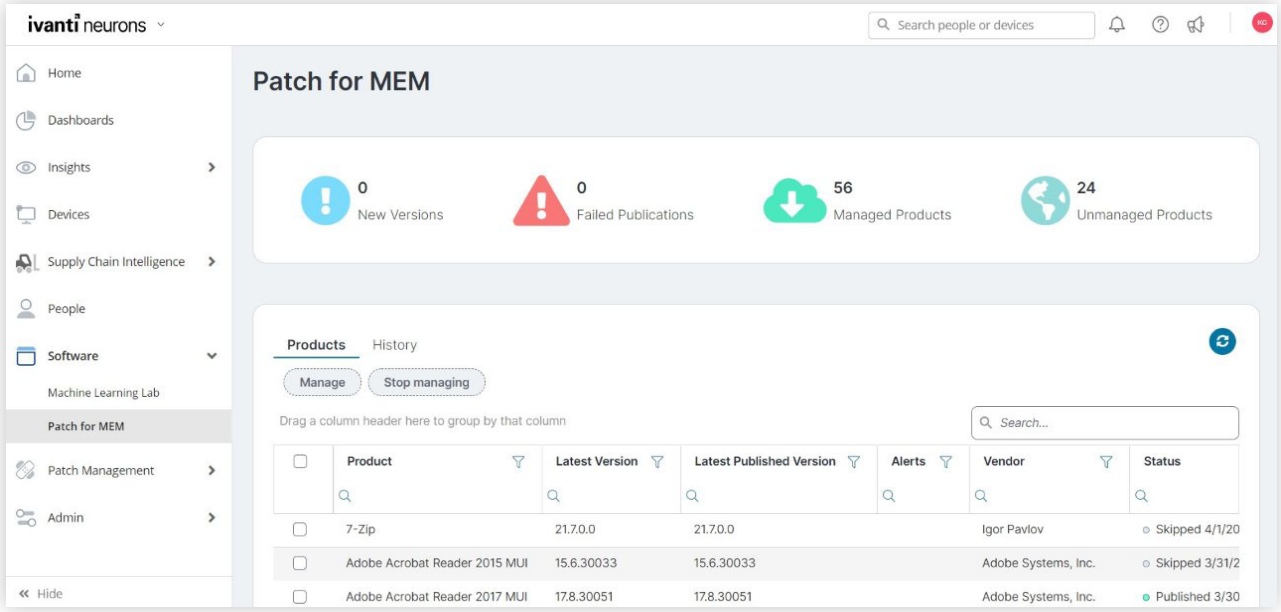
Ivanti Neurons Patch for MEMは、既存のMicrosoft Intuneの実装を拡張して、サードパーティ製アプリケーションをアップデートします。脅威およびパッチインテリジェンスにより、企業はサードパーティ製ソフトウェアの脆弱性修復を的確に優先順位付けできます。

Intuneでのサードパーティのアップデート

データ侵害とランサムウェア攻撃は、年を追うごとに増加しています。同様に、企業が導入するアプリケーションの数も増加傾向にあり、2016年から24%増加しています*[1]。このため、サードパーティアプリケーションがサイバー攻撃者にとって恰好の攻撃ベクトルの1つになっていることは当然と言えるでしょう。残念ながら、サードパーティアプリケーションの脆弱性に起因する情報漏洩は被害が最も高額なものの一つで、企業の平均被害額は433万ドルとなっています*[2]。

このため、企業はサードパーティアプリケーションのアップデートに積極的に取り組む必要がありますが、管理すべきアプリケーションの数が増え続けているため、それも困難な状況にあります。さらに問題を複雑にしているのは、追跡しなければならない脆弱性の数が増加していることです。全米脆弱性データベース（NVD）では、1日平均61件の脆弱性が公開されています*[3]。

良い点としては、CVE（共通脆弱性識別子）のうち、広く悪用されているのはわずか4%であることです*[4]。しかし、NVDに登録されている13万件を超える脆弱性の中から、その4%を特定することは困難です。例えば、企業がCVSS（共通脆弱性評価システム）v3 に基づいて重大な脆弱性をすべてパッチしたとしても、ランサムウェアの脆弱性の73.61%にはパッチを当てられていないことになります*[3]。



このような状況は、Microsoft Intuneを活用してアプリケーションやアップデートをデバイスに配信している企業にとって、さらに問題が大きくなる可能性があります。Intuneは、Microsoftのアプリケーションに対して包括的なパッチ管理機能を提供していますが、サードパーティのアプリケーションをアップデートするためのネイティブな機能はありません。

Ivanti Neurons Patch for MEMについて

Ivanti Neurons Patch for MEMは、既存のMicrosoft Intuneの実装を拡張して、インフラを追加することなくサードパーティのアプリケーションをアップデートします。実用的な脅威インテリジェンスとパッチの信頼性に関するインサイトを提供し、企業に最も危険を及ぼす脆弱性をIT部門が優先的に修正できるようにします。Ivanti Neurons for Patch for MEMにより、企業はデータ漏洩やランサムウェア、その他サードパーティのアプリケーションの脆弱性に起因する脅威から自らを守ることができます。

主な機能と特徴

サードパーティーのパッチパブリッシングでMicrosoft Intuneを拡張

サードパーティアプリケーションの脆弱性に起因する脅威から保護すると同時に、Intuneへの投資効果を最大化します。Ivanti Neurons Patch for MEMは、IvantiのNeuronsクラウドプラットフォームから、テスト済みのサードパーティアプリケーションのアップデートをIntuneに直接パブリッシュします。これにより、IT部門が既存のアプリケーションライフサイクル管理ワークフローの一部として、Intune内のMicrosoft OSおよびアプリケーションアップデートと同時にサードパーティ製アプリケーションのアップデートを展開できるようにします。

また、Ivanti Neurons Patch for MEMはクラウドネイティブソリューションであるため、Intuneユーザーが、パッチのワークロードを完全にクラウドに移行して、インフラを追加することなくMicrosoftのビジョンであるモダンマネジメントを実現できるよう支援します。

アクティブなエクスプロイトに対するプロアクティブな保護

ランサムウェアに関連するものを含む脆弱性に対する既知のエクスプロイトと脅威コンテクストのインテリジェンスにより、敵対的リスクに基づく修復の優先順位付けを行います。Ivantiの脆弱性リスク評価（VRR）は、最も忠実性の高い脆弱性と脅威のデータに加え、ペネトレーションテストチームによるエクスプロイトの人的検証を取り入れることで、基本のCVSSスコアリングよりもリスクに応じた優先順位による対策を講じることができます。

パッチ展開の失敗を回避

事前テスト済みのアプリケーションのアップデートとパッチの信頼性インサイトにより、時間を短縮しながらパッチ展開の失敗を回避します。Ivantiは、作成したパッチコンテンツのパッケージに対し徹底的にテストを行っています。テストは広範な仮想環境で行われ、製品としてリリースされる前に、パッケージがさまざまなアプリケーションのバージョンとオペレーティングシステムで動作することを確認します。

さらに、クラウドソーシングによるソーシャルセンチメントデータおよび匿名化パッチ展開テレメトリからのパッチの信頼性に関するインサイトで、アプリケーションアップデートを展開する前に実環境での信頼性に基づいたアップデート評価ができるようになります。

パッチ管理プロセスの合理化

Ivanti Neurons Patch for MEMの優れた機能が、様々な業務の効率性を実現します。

- サードパーティアプリケーションのアップデートが利用可能になると、Intuneに自動でパブリッシュします（自動パブリッシュはオプション）。
- 事前テスト済みアプリケーションアップデートとパッチの信頼性に関するインサイトにより、より信頼性が高く失敗の少ないパッチ適用を実現します。
- 脅威インテリジェンスにより、パッチ適用を効果的に優先順位付けし、IT部門が重要な仕事に集中できるようにします。
- エクスプロイトやマルウェアのインサイトにより、セキュリティチームとITオペレーションチーム間のデータとリスクに関するコミュニケーションを促進し、オペレーションの協調性を向上させます。

Ivantiについて

Ivantiは「Everywhere Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない働き方により、従業員は多種多様なデバイスでさまざまなネットワークからITアプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons自動化プラットフォームは、業界をリードする統合エ ンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの 自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合ITプラットフォームを提供します。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまでIT資産の管理、検出、保護、サービスのためにIvanti を選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験を提供しています。詳細については、www.ivanti.co.jp をご参照ください。

ivanti

ivanti.co.jp
03-6432-4180
contact@ivanti.co.jp

1. Okta「Business at Work 2022 Report」（2022年） https://www.okta.com/report/businesses-at-work-2022/
2. IBM Security「2021 Cost of a Data Breach Report」2021年7月28日 https://www.ibm.com/security/data-breach
3. Cyber Security Works, Cyware, Ivanti「2022 Ransomware Spotlight Report」2022年1月26日 https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report
4. Cybersecurity and Infrastructure Security Agency (CISA)「Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities」2021年11月3日 https://cyber.dhs.gov/bod/22-01/