継続的な脆弱性管理

攻撃者によって組織の IT インフラストラクチャの弱点が悪用されると、金銭上の損害だけでなく、生産性と評判も大きく損なわれる可能性があります。サイバーセキュリティを継続的なプロセスとしてとらえないと、お客様のチームが脆弱性にパッチを適用できるよりも早く、ハッカーによってお客様のインフラストラクチャの脆弱性が発見され、兵器化、展開、攻撃が行われて、インフラストラクチャがリスクにさらされるかもしれません。お客様のシステムが今日安全だとしても、来週には攻撃者が環境内に存在する重大な脆弱性を発見して悪用する可能性があります。

米国の CIS (Center for Internet Security) は、継続的な脆弱性管理を「脆弱性を特定し、修正を行い、攻撃者にとっての攻撃の機会を最小限に抑えるため、新しい情報を継続的に取得して評価し、措置をとること」と説明しています。

組織のセキュリティ プラクティスの一環として継続的な脆弱性管理を実施すべきですが、脆弱性が初めて特定されてからソフトウェア更新プログラムが展開されるまでにかかる時間と手作業が課題となっています。レポートとレポートの合間に盲点ができるのを防ぐには、脆弱性のスキャンを頻繁に行うことからこのプロセスを始めることが推奨されます。

セキュリティ チームが脆弱性データを取得して優先順位を付け、それを IT チームに提供すると、IT チームはそれらの共通脆弱性識別子 (CVE) をソフトウェア更新プログラムに転換して、どのタイトルを更新すべきか優先順位を付ける必要があります。脆弱性が 1 つなら簡単に特定して修正することができますが、検出された CVE が 1 万件やさらには 10 万件だったらどうなるでしょうか。

1 回の脆弱性評価で、環境内の複数のシステムに同じ問題が見つかる場合があります。また、同じ脆弱性が 1 つのシステム上の多数のソフトウェアで見つかることも考えられます。CVE を重複除去および調査し、各脆弱性を解決するために必要な措置を明らかにするには、このプロセスを行うたびに 5 ～ 8 時間程度かかる可能性があります。1 日ぐらい大したことはないように思われるかもしれませんが、脆弱性の悪用のほとんどが更新プログラムの提供開始から 14 ～ 28 日以内に行われることを考えると、1 日遅れるごとに攻撃者に足掛かりを得る時間をより多く与えることになります。

脆弱性の特定からパッチの展開までの時間を短縮

Ivanti のセキュリティソリューションを使用すると、より良い洞察を得て、セキュリティ体制を強化できます。エンドポイントとサーバーへのパッチの適用が自動化されるため、オペレーティングシステムとサードパーティ製アプリケーション全体に常に最新のパッチを適用できます。弊社のパッチ適用ソリューションは、脆弱性スキャナー、構成管理ツール、およびレポート作成機能を統合して、IT チームとセキュリティ チームの時間を最適化します。

継続的な脆弱性管理を実現

Ivanti のセキュリティ ソリューションは、脆弱性を特定、分類し、それらに対処する一連のプロセスを合理化して、セキュリティ脆弱性レポートから修正までの時間のギャップが攻撃者に悪用されるのを防ぎます。IT チームは、セキュリティ チームが取得した脆弱性スキャン結果を容易にインポートできます。特定された CVE と関連するパッチを素早く確認し、漏れているパッチがあれば展開対象として公開または承認し、時間を大幅に節約できます。

Ivanti Patch for SCCM と Ivanti Patch for Endpoint Manager のどちらでエンドポイントにパッチを適用する場合でも、あるいは Ivanti のセキュリティ ソリューションでデータセンターにパッチを適用する場合でも、お客様は CVE を特定してパッチを適用する機能を利用できます。

IT チームがこれまで何時間もかけて手作業で重複除去と調査を行って更新プログラムのパッチ グループを準備していた場合、IT チームのエクスペリエンスと生産性を向上させることができます。脆弱性管理ベンダーからのリストを任意の形式 (CSV、XML、またはプレーンテキストファイル) で簡単にインポートすることが可能です。続いて CVE を特定の脆弱性に対応する適切なソフトウェア更新プログラムに自動的にマッピングして、どのパッチを適用する必要があるか素早く可視化します。環境内で承認された更新プログラムのパッチ グループを作成して、さらに各パッチに関連するすべての情報を確認することもできます。

より良い洞察を得て、セキュリティ体制を強化

IT チームは、パッチの調査、テスト、展開を行うのに何日かかり、それらのパッチをどのように優先順位付けしていますか。ブログ記事やベンダーのドキュメントなどのソースから既知の問題を調査して、パッチ更新プログラムの信頼性を見極めることも、時間のかかるもう 1 つの作業です。また、活発に悪用されているものではなく重大なパッチを展開することを現在の経験則としている場合は、パッチの優先順位を付けることでリスクが高まることも考えられます。

どのパッチの優先順位付け、テスト、および展開を行うかによっては、脆弱性管理プロセスが長引く可能性があります。お客様は、Ivanti のサードパーティ パッチ カタログと、パッチの信頼性およびセキュリティの指標とを結び付ける Patch Intelligence ツールをご利用いただけます。弊社のツールがなければ時間と手間のかかる洞察を得られるようになり、最も重要な更新プログラムの展開を最適化できます。

- **可視化**：特定のパッチまたはパッチ グループに対してベンダーから報告される問題や、Ivanti によって関連する CVE とパッチと共に指定された掲示板情報で特定される問題を可視化します。
- **洞察の拡大**：パッチをロールバックする必要があったかどうかの報告を返す匿名化されたピア データによって、Ivanti の複数のお客様が経験された問題へと洞察を拡大します。
- **信頼性の判断**：迅速な展開を行う際に、更新プログラムの信頼性と信頼レベルを判断します。
- **パッチの特定**：さらなるテストが必要なパッチと、成功の確率が高いファストトラック パッチを特定します。これにより、脅威スコアと信頼性評価に基づいてテストの優先順位付けと即時展開可能なパッチの優先順位付けを行った上で、ロールアウトしてパッチ サイクルを最適化できるようにします。

Ivanti の継続的な脆弱性管理ソリューションによって、攻撃者の先を行きましょう。詳細については、sales@ivanti.com までお問い合わせください。

詳細

ivanti.co.jp
03-5226-5960
Contact@ivanti.co.jp