ivanti

データ シート

CVE を特定してパッチを適用する リスクベースの承認

Ivanti パッチ管理ソリューションで利用可能

Ivanti は、脆弱性スキャン結果を読み込み、特定された共通脆弱性識別子 (CVE) と関連するパッチを確認し、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する機能を提供します。

おそらくお客様の IT 運用チームと IT セキュリティ チームは「異なる言語を話している」のではないでしょうか。それは、IT 運用チームが物事を円滑に進める必要があるのに対し、セキュリティ チームは環境を保護する義務があるためです。しかし、どちらのチームも「ビジネスを保護し、ビジネスの能力を高める」という共通目標を共有しています。そしてこの目標を達成する上で両チームが協力して取り組む必要がある場所が、エンドポイントです。

継続的な脆弱性の評価と修正

どの組織でも、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の評価と修正を間違いなく実施すべきですが、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大きな負担になっています。

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、セキュリティ チームから提供される脆弱性レポートではたいてい 1,000 件以上の CVE が検出されているはずです。しかし、それが 1 万件やさらには 5 万件だったらどうなるでしょうか。1 回の脆弱性評価で、環境全体の複数のシステム上で複数の問題が見つかる場合があります。また、同じ脆弱性が多数のシステムで見つかったり、同じシステム上の多数のソフトウェアで見つかったりすることも考えられます。

評価と修正の取り組みは瞬く間に複雑で時間のかかる作業になります。そうなれば、攻撃者がその隙をついて機密データにアクセスする足掛かりを得ようとする可能性があります。選別と計画に時間がかかるほど、セキュリティ インシデントへと発展しやすくなるのです。IT 運用チームはセキュリティ チームから提供される脆弱性レポートを精査し、CVE を特定していずれかの更新プログラムと対応付け、それらをパッチ管理ソリューションによって展開する必要があります。

CVE の特定からパッチの適用までの時間を短縮

Ivanti ソリューションに搭載された、CVE を特定してパッチを適用するためのインポート機能を利用すれば、このプロセスを数時間から数分にまで合理化できます。Rapid 7、Tenable、Qualys、BeyondTrust など、どのベンダーの脆弱性評価を使用しているかにかかわらず、Ivanti ソリューションはそれらの CVE に関連するパッチをマッピングして、更新プログラムのパッチ リストを作成します。このリストを素早く承認または公開して、環境内で修正を行うことができます。

特定された CVE 情報はインポートされます。Ivanti のパッチ ソリューションは、この情報を抽出して、CVE を、脆弱性を解決するために必要なソフトウェア更新プログラムにマッピングします。

次に、CVE を特定して、個々の特定の脆弱性を解決する更新プログラムと対応付け、エンドポイントにどのパッチを適用する必要があるかを正確に示すことができます。

例えば、環境全体で検出された 40 万件の脆弱性が含まれる脆弱性レポートがあるとします。レポートの一意の CVE ID をすべて手作業で重複除去して調査するプロセスには、数時間あるいは数日かかることもあり得ます。Ivanti ソリューションを使用して CVE とパッチをマッピングすれば、セキュリティ チームから新しいレポートが運用チームに提供されるたびに、その時間と労力を数分にまで短縮できます。

これらの機能の詳細については、
Contact@ivanti.co.jp までお問い合わせください。

詳細 ivanti.co.jp 03 5223 59630 Contact@ivanti.co.jp