ivanti

Vulnerability Risk Rating（VRR）/脆弱性リスク評価
敵対的リスクの測定

Ivantiは、Vulnerability Risk Rating（以下、VRR）に脅威の状況を取り込むことにより、ホストとアプリケーションで発見される全ての結果において、潜在的な侵害の重要な指標となる脆弱性に一貫した優先順位を付けることができます。

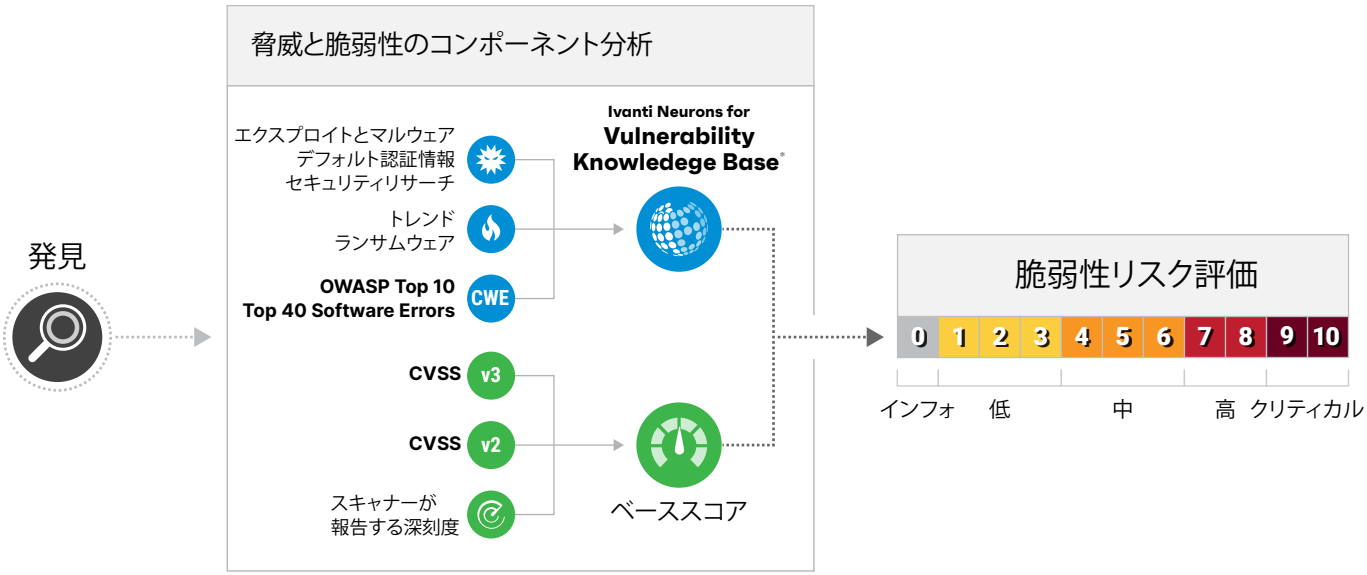
Vulnerability Risk Rating/脆弱性リスク評価とは？

VRRは、業界標準の**CVSS**（**Common Vulnerability Scoring System**）、**CWE**（**Common Weakness Enumeration**）データ、**OWASP**（**Open Web Application Security Project**）、オープンソースの脅威インテリジェンス、専門知識、トレンド情報などを考慮したものです。**VRR**は、ある脆弱性が組織やビジネスにもたらすリスクを表すもので、**0~10**の間の数値スコアとして提供されます。リスクが高いほど**VRR**も高くなります。

個々の脆弱性にVRRを割り当てるために、Ivanti Neuronsは脆弱性の脅威要因を特定し、基本スコアを決定します。エクスプロイトやマルウェア、脅威のトレンドランサムウェア、セキュリティリサーチなどのパラメータは、Ivanti Neurons for Vulnerability Knowledge Baseと呼ばれる統一された独自のデータベースに関連付けられ、正規化されます。利用可能な脅威インテリジェンスに関連する最大のリスクは、方程式に組み込まれます。

VRRを計算する次のステップは、基本スコアの割り当てです。Ivantiは、CVSS v3が利用可能な場合はこれを利用し、v3が提供されていない場合は、CVSS v2で代用します。脆弱性にCVEの関連付けがない場合は、0から10までのスケールで正規化されたスキャナーから報告された深刻度が使用されます。

VRR計算手法の最終ステップは、すべてのパラメータを一連のデータ駆動型アルゴリズムに渡し、各パラメータ値を対応する数値にマッピングし、マッピングされた値を使用して明示的なVRRを計算することです。各脆弱性のリスク評価は、その数値に応じてクリティカル（Critical）、高（High）、中（Medium）、低（Low）、インフォメーショナル（Informational）のいずれかの深刻度に分類されます。



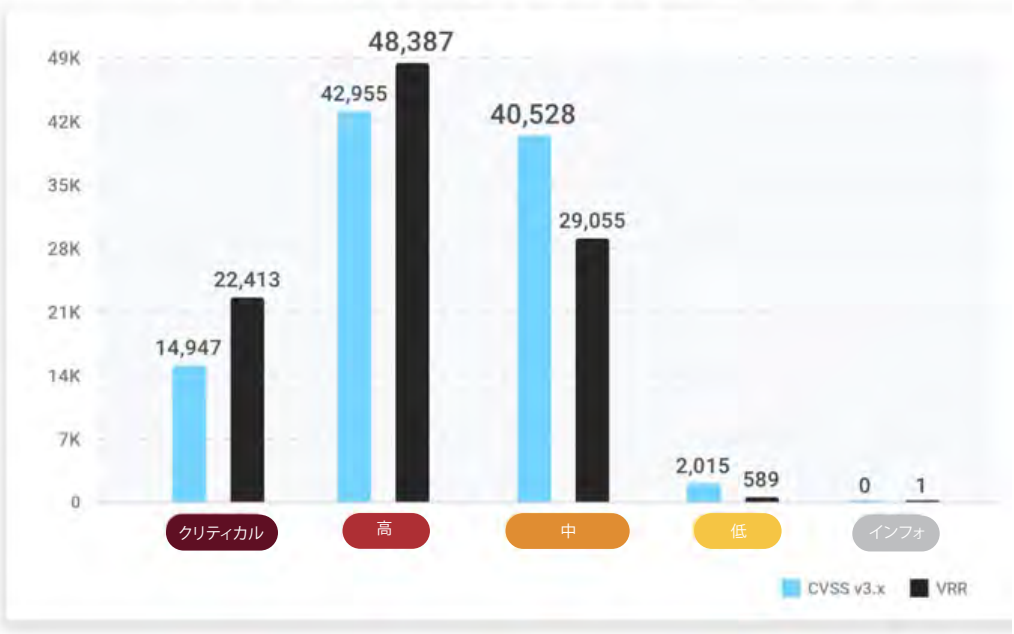
このスコアは、Ivanti Neuronsに加え、ネットワークスキャナやアプリケーションスキャナによって収集された標準化されたメトリクッスとナレッジを活用することで、敵対的なリスクを定量化します。Ivanti Neuronsは、トレンドのエクスプロイト情報やIvantiが特定した脅威を含む、100を超えるソースからのタイムリーな脅威インテリジェンスの集合体です。包括的な脅威インテリジェンスは、脆弱性情報と関連付けられ、インテリジェントなスコアリングと優先順位付けのための豊富なコンテキストを提供します。さらに、NVD（National Vulnerability Database）、2021年CWE Top 40 Most Dangerous Software Errors、2021年OWASP Top 10などの業界標準のソースと、ペネトレーション・テスターの専門知識を組み合わせて、スコアリング・アルゴリズムに情報を提供するためのデータ駆動型モデルを構築します。

VRRは他のスコアリング方法とどう違うのか？

CVSSだけでは、脆弱性がもたらすリスクの全体像を把握することはできません。NVDが脆弱性を公表してからCVSSを公開するまでにはタイムラグがあります。Ivanti Neuronsは、このギャップを埋めるためにCNA（CVE Numbering Authority）からデータを収集し、一般には公開されていない新たに検証されたエクスプロイトについて、業界をリードするセキュリティ研究者から直接情報を得ます。さらに、キュレーションされた脅威フィードは、広範なカバレッジを提供し、実際に使用されているトレンドのエクスプロイトに関する継続的なアップデートを提供します。これにより、VRRは、脅威の相関性により、CVSSよりも優位に立つことができます。

アプリケーションの脆弱性を定量化することはさらに難しく、CVEと関連付けられるものはほとんどありません。このような場合は、アプリケーションの脆弱性に適したCWEやOWASPを使用することになります。CWEには標準化されたスコアが提供されているものもあれば、そうでないものもあります。VRRは、スキャナー情報とIvanti Neuronsの組み合わせを利用することで、これらの矛盾に対処し、これらのアプリケーションの弱点に関する視野を広げ、それぞれの弱点についてより大きなコンテキストを構築します。VRRのアルゴリズムは、基本レベルのスコアを分類的に上昇させるのではなく（リスクインフレを招く）、最もリスクの高い弱点をインテリジェントに分離して引き上げ、正確で実用的なスコアで効果的に優先順位を付けることができます。

脆弱性カウント、**CVSS v3** 対 **VRR** 2022年3月9時点



なぜ**VRR**の利用を検討すべきなのか？

VRRはプロアクティブに、ダイナミックに、タイムリーに、全体を見通せます。

VRRは、インフラとアプリケーションを横断して発見された情報を比較するユニークな方法を提供します。ほとんどの組織では通常、Common Vulnerabilities and Exposures（CVE）またはCommon Weakness Enumerations（CWE）のいずれかを共通のベースとして使用しています。脆弱性修正戦略を改善するために、組織は影響を正確に測定し、脆弱性が悪用される可能性を判断する必要があります。Ivanti Neuronsは、脅威インテリジェンスとヒトの認識を考慮し、組織に各脆弱性の完全なコンテキストを理解させることで、脆弱性をアクション可能なものにします。

Ivanti Neuronsは、スキャナーの詳細情報、CVSS、オープンソースの脅威インテリジェンスなど、既存のツールやデータも活用します。しかし、発見されたものに明らかな脅威が関連付けられていない場合、Ivanti Neuronsは、CWE Top 40 Software ErrorsやOWASP Top 10などの業界が推奨するリストを活用することで、そのギャップを埋め、リスクを計算する際に追加のコンテキストを提供します。リスクの可能性をさらに絞り込むために、Ivanti NeuronsはCVEを脅威インテリジェンスと相互に関連づけて、発見された情報にさらに優先順位付けをおこないます。

組織は、修復の優先順位をつけるために、脆弱性に関するより詳細な調査目線での見解を必要としています。VRRを使用することで、ネットワーク・インフラストラクチャとアプリケーションの脆弱性管理を最適化することができます。

CVE-2017-0144を例に見てみましょう。この脆弱性はWannaCryの一部であり、ランサムウェアに関連しています。さらに、関連する弱点がTop 40とOWASP Top 10のリストにも入っています。この脆弱性のベーススコアはHigh: 8.1ですが、Ivanti Neuronsはその知名度の高さと脅威を考慮し、Critical: 10に再分類しています。

VRRによるスコアリングの例

CVE	CVSS	エクスプロイト	CWE	OWASP Top 10	CWE Top 40	VRR	概要
CVE-2019-0708	9.8	Yes	416	No	Yes	10	この脆弱性は**BlueKeep**の一部であり、関連するランサムウェアだけでなく、関連するCWEもトップ40にランクインしています。
CVE-2021-45105	5.9	Yes	20	Yes	Yes	7.47	この脆弱性は**Log4j**の一部であり、関連するDoSだけでなく、OWASPトップ10リストに該当する関連するCWEもあります。
CVE-2019-3978	7.5	Yes	306	Yes	Yes	8.24	この脆弱性はアタックサーフェス（**Attack Surface) – RS**の一部であり、エクスプロイト情報が公開されています。OWASP Top 10リストに該当する関連する弱点は、VRRを増加させるが「高」に分類されています。
CVE-2020-4430	4.3	No	22	Yes	Yes	6.17	この脆弱性は**CISA Known Exploited**の一部であり、利用可能な既知のエクスプロイト情報はありません。しかし、関連するOWASP Top 10 は、CVSSと同じ分類に留まりながら、より多くのコンテキスト情報を追加しています。
CVE-2017-0143	8.1	No	20	Yes	Yes	10	この脆弱性は、**MS17-10** に関連し、RCE、ランサムウェア、OWASP に関連しています。NVDはこの脆弱性を「高」の上位に評価していますが、Ivanti Neurons は、OWASP Top 10 および CWE Top 40 に関連する脆弱性があるため、この脆弱性を「クリティカル」と評価しています。

Ivantiについて

Ivantiは、ITとセキュリティの垣根を取り払いEverywhere Work（場所にとらわれない働き方）を実現します。IvantiのCIOとCISO向けに特化したプラットフォームは、ITとセキュリティのチームに、組織のニーズに合わせて拡張できる包括的なソフトウェアソリューションを提供し、セキュアに従業員体験を向上させます。Ivantiプラットフォームは、クラウドスケールのインテリジェントなハイパーオートメーションレイヤーであるIvanti Neuronsを搭載しており、組織全体でプロアクティブな修復とユーザーフレンドリーなセキュリティを実現し、ユーザーが満足するような従業員体験を実現します。Ivantiのエンドツーエンドのソリューションは、Fortune 100社のうち85社を含む40,000社以上の顧客によって採用されています。Ivanti は、すべての視点が聞き入られ、尊重され、評価される環境づくりに尽力し、顧客、パートナー、従業員そしてよりサステイナブルな未来の実現するために取り組んでいます。ivanti.com/ja

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