Vulnerability Risk Rating

Measuring Adversarial Risk

By capturing threat context in our Vulnerability Risk Rating, Ivanti is able to consistently prioritize vulnerabilities that are key indicators of potential compromise across host and application findings.

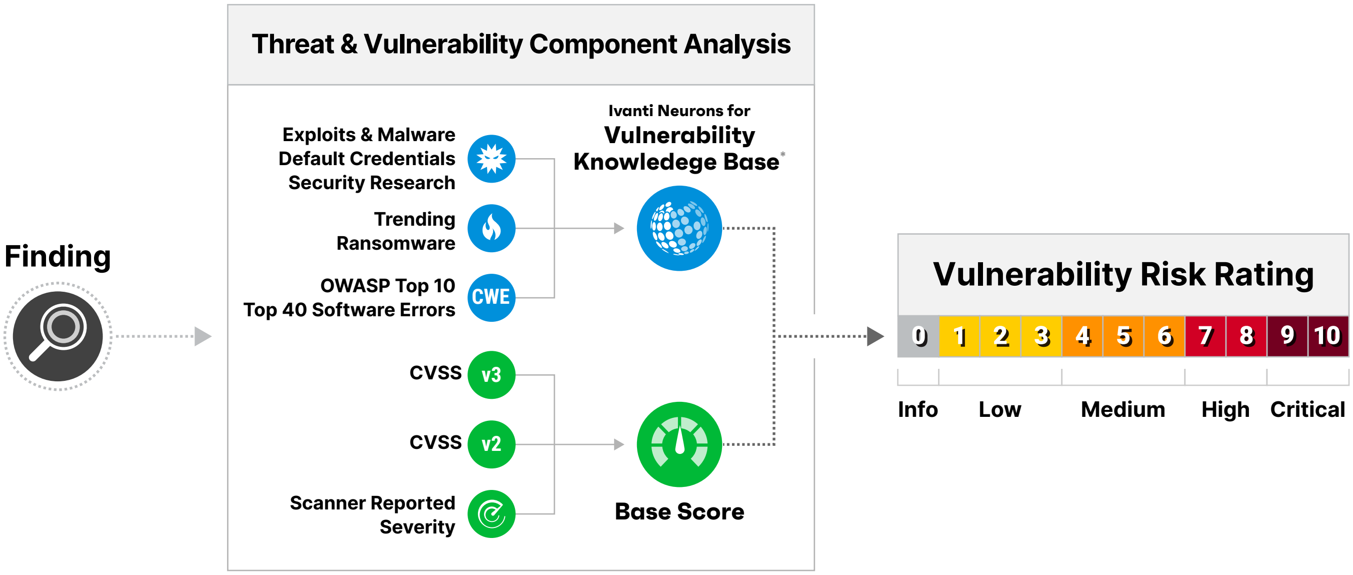
What is Vulnerability Risk Rating?

Vulnerability Risk Rating (VRR) considers industry-standard Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE) data, OWASP (Open Web Application Security Project), open-source threat intelligence, subject matter expertise, trending information, and more. VRR represents the risk posed by a given vulnerability, provided as a numerical score between 0 and 10, to an organization or business. The higher the risk, the higher the VRR.

To assign a VRR to an individual vulnerability, Ivanti Neurons identifies the vulnerability's threat factor and determines the base score. Parameters such as Exploits and Malware, Trending Threats, Ransomware, and Security Research are correlated and normalized into a unified proprietary database known as the Ivanti Neurons for Vulnerability Knowledge Base. The greatest risk associated with the available threat intelligence is factored into the equation.

The next step in computing VRR is the assignment of the base score. Ivanti utilizes the CVSS v3 where available, and substitutes the CVSS v2 when v3 is not provided. If a vulnerability lacks a CVE association, the scanner reported severity normalized on a scale from 0 to 10 is used.

The final step in the VRR calculation methodology is to pass all the above parameters into a sequence of data-driven algorithms that map each parameter value to a corresponding numerical value, and then compute the explicit VRR using those mapped values. Each vulnerability's risk rating lies within one of a set of severity groups according to its numerical value: Critical, High, Medium, Low, or Informational.



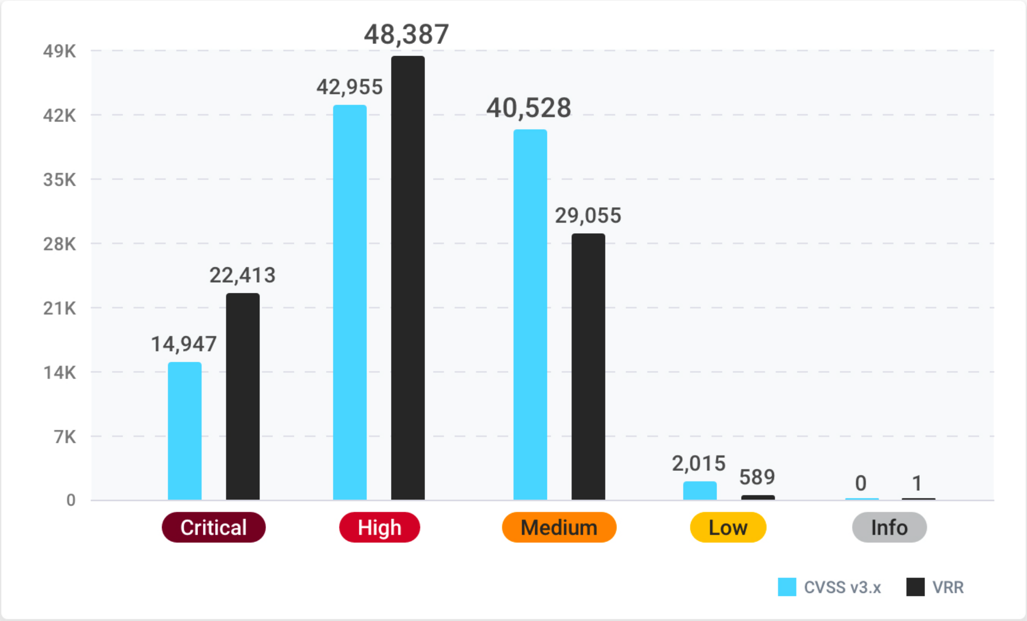
The score quantifies adversarial risk by leveraging standardized metrics and knowledge gathered by network and application scanners, in addition to Ivanti Neurons. Ivanti Neurons is an aggregate of temporal threat intelligence from over 100 sources, including trending exploit information and Ivanti-identified threats. The comprehensive threat intelligence is then correlated to vulnerability information, providing a rich context for intelligent scoring and prioritization. Additionally, industry-standard sources such as the NVD (National Vulnerability Database), the 2021 CWE Top 40 Most Dangerous Software Errors, and the 2021 OWASP Top 10 are combined with subject matter expertise from penetration testers to build data-driven models used to inform the scoring algorithm.

How does Vulnerability Risk Rating differ from other scoring methods?

The CVSS alone cannot provide a complete picture of the risk posed by a vulnerability. There is often a lag in which the NVD can publish a vulnerability and publish a CVSS. Ivanti Neurons gathers data from CNAs (CVE Numbering Authority) to bridge that gap, along with direct input from industry-leading security researchers about newly validated exploits that are not publicly available. In addition, curated threat feeds provide broad coverage and continuous updates on trending exploits actively being used in the wild. This gives VRR a superior edge against CVSS due to the correlation of threats as compared to solely severity.

Application vulnerabilities are even more challenging to quantify, with very few being associated with CVEs. In these instances, we rely instead on CWEs and OWASP, which are more appropriate for application weaknesses. Some CWEs are provided standardized scores, while others are not. VRR utilizes a combination of scanner information and Ivanti Neurons to address these inconsistencies and to widen the lens on these application weaknesses, building a larger body of context for each one. Rather than categorically increasing base level scores (resulting in risk inflation), the VRR algorithm intelligently separates and elevates the riskiest weaknesses, allowing you to prioritize effectively with accurate and actionable scores.

Vulnerability Count, CVSS V3 vs VRR as of March 9, 2022



Why should I consider using Vulnerability Risk Rating?

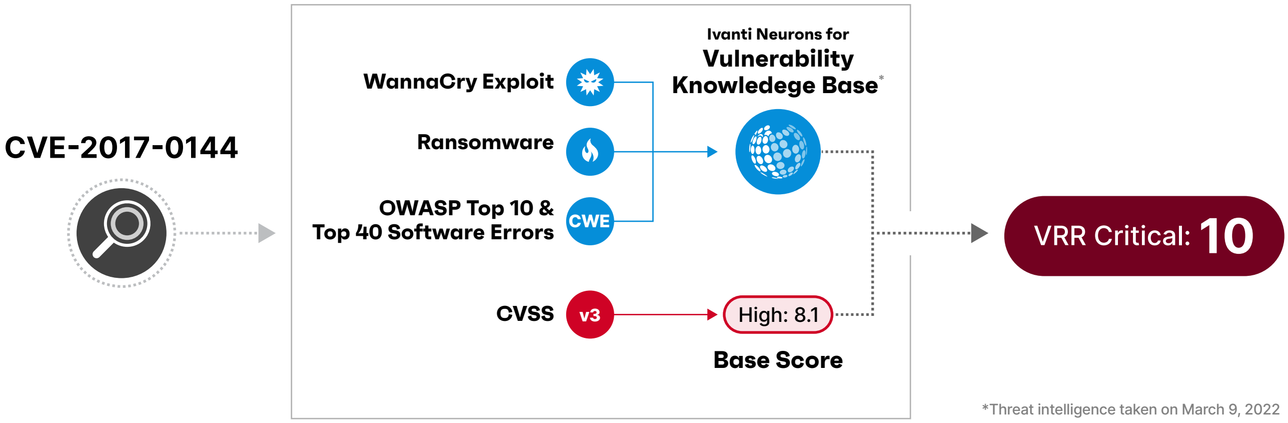
VRR is proactive, dynamic, temporal, and comprehensive.

VRR provides a unique way to compare finding information across infrastructure and applications. Most organizations typically use either Common Vulnerabilities and Exposures (CVEs) or Common Weakness Enumerations (CWEs) as a common base. In order to improve vulnerability remediation strategies, organizations need to accurately measure impact and determine the likelihood that a vulnerability will be exploited. Ivanti Neurons makes vulnerabilities actionable by factoring in threat intelligence and human cognition, giving organizations a thorough understanding of the full context of each vulnerability.

Ivanti Neurons also leverages existing tools and data, such as scanner details, CVSS, and open-source threat intelligence. However, in instances where no obvious threat is associated with the finding, Ivanti Neurons fills that gap by leveraging industry-endorsed lists, such as the CWE Top 40 Software Errors and OWASP Top 10, to provide additional context when calculating risk. To further refine the risk likelihood, Ivanti Neurons cross-correlates CVEs with its threat intelligence to further prioritize findings.

Organizations require an in-depth, research-driven view of vulnerabilities if they are to prioritize remediation. They can use VRR to optimize the vulnerability management of their network infrastructure and applications.

Let us take **CVE-2017-0144** as an example. This vulnerability is a part of WannaCry and is associated with ransomware. In addition, an associated weakness falls on the Top 40 and OWASP Top 10 lists as well. Although the vulnerability has a base score of High 8.1, Ivanti Neurons factors in its high profile and threat exploits and reclassifies it at a Critical 10.



*Threat intelligence taken on March 9, 2022

A couple of other examples of the value added by VRR are captured in the table below:

CVE	CVSS	Exploit	CWE	OWASP Top 10	CWE Top 40	VRR	Description
CVE-2019-0708	9.8	Yes ✸	416	No	Yes ✓	10	This vulnerbility is a part of **BlueKeep** and not only has an associated ransomware but also an associated CWE on the Top 40 list.
CVE-2021-45105	5.9	Yes ✸	20	Yes ✓	Yes ✓	7.47	This vulnerbility is a part of **Log4j** and not only has an associated DoS, but also an associated CWE that falls on the OWASP Top 10 list.
CVE-2019-3978	7.5	Yes ✸	306	Yes ✓	Yes ✓	8.24	This vulnerbility is a part of **Attack Surface – RS** with exploit information available. An associated weakness that falls under the OWASP Top 10 list increases VRR but stays within the High band.
CVE-2020-4430	4.3	No	22	Yes ✓	Yes ✓	6.17	This vulnerbility is a part of **CISA Known Exploited** and has no known exploit information available. However, an associated OWASP Top 10 adds more context to the picture while staying within the same band as CVSS.
CVE-2017-0143	8.1	No	20	Yes ✓	Yes ✓	10	This vulnerability is associated to **MS17-10** and has an associated RCE, ransomware, and OWASP. While NVD scores this vulnerability on the upper band of High, Ivanti Neurons scores it as Critical because there is an associated weakness on the OWASP Top 10 and CWE Top 40.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti
ivanti.com
1 800.982.2130
sales@ivanti.com