Cisco Vulnerability Intelligence

Enhance your VM workflows with rich vulnerability intel

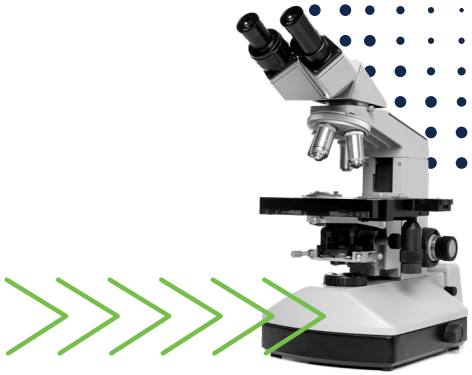
Cisco Vulnerability Intelligence gives security teams access to the industry's richest consolidation of vulnerability intel via an API. Cisco Vulnerability Intelligence incorporates rich CVE data from more than 19 threat and exploit intel feeds, including custom-curated sources. Organizations can access these records via an API to use within their existing vulnerability management (VM) workflows, or they can search and review CVE data within a user interface (UI).

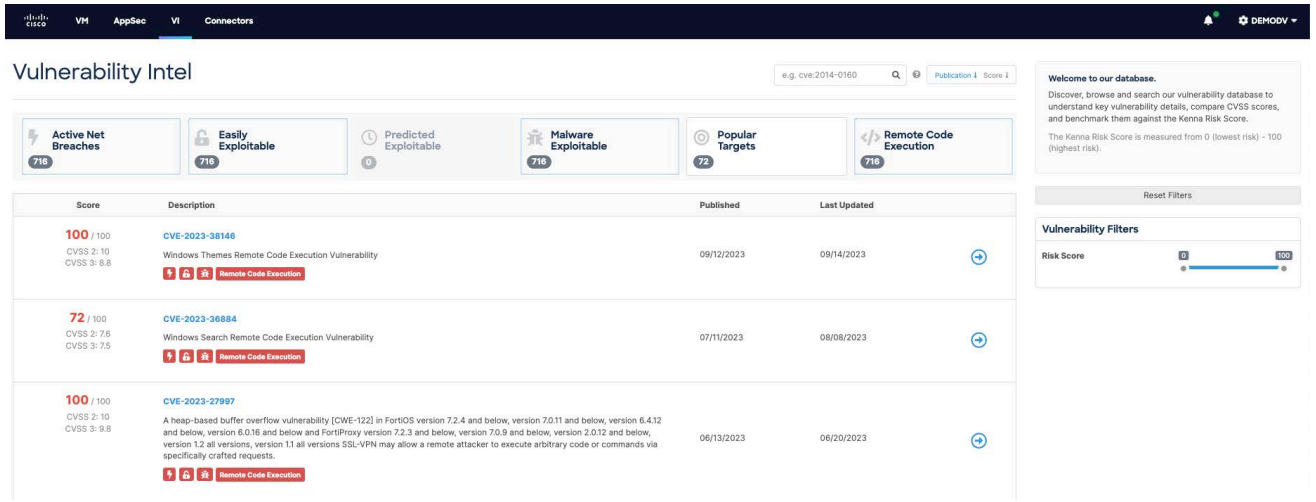
Benefits

- **Gather intel on any CVE** to understand what risk it may pose to your organization, and how to prioritize your remediation efforts.
- **Query and export CVE records** to understand how attackers can exploit CVEs in the real world and inform your defense measures.
- **Overlay your existing data sources** with Cisco's unique vulnerability intel to add additional context around CVEs.
- **Integrate Cisco Vulnerability Intelligence** into any VM workflow and maximize the ROI of your existing VM solution deployment(s).
- **See the Cisco Security Risk Score and predicted exploitability** of all CVEs—unique data points derived from Cisco Vulnerability Management's machine learning—for a greater level of vulnerability insight and prioritization.

Research CVEs in a Simple UI

Cisco Vulnerability Intelligence gives security teams access to the industry's richest consolidation of vulnerability intel via an easy-to-use UI. With Cisco Vulnerability Intelligence security researchers can look up CVEs (irrespective of scanner findings in their organization) and find out critical information and answer important questions like: Are there fixes available for this specific vulnerability? Is it being used in any real-world breaches?





The Cisco Vulnerability Intelligence user interface (UI)

Examples of Cisco Vulnerability Intelligence CVE Data	
Popular Target	If a vulnerability is trending across Cisco Vulnerability Management's customer base
Risk Score	Cisco Security Risk Score (1–100)
Remote Code Execution	If a CVE is capable of being exploited remotely
Predicted Exploitable	If Cisco Vulnerability Intelligence predicts future exploits to develop that leverage a CVE
Active Internet Breach	If Cisco Vulnerability Intelligence sees this vulnerability definition in trending breach activity
CVSS and CVSS v3 Score	Base score from CVSS and CVSS Version 3
Easily Exploitable	If the vulnerability is included in a known exploit kit or public exploit source
Exploits	Information on exploits, such as the data source's external ID and name for the exploit and a timestamp of when the exploit was created.
Fixes	Information on fixes, such as a URL to fix explanation(s), the product to which the fix applies, and more.
Malware	Known MD5 hashes of common malware using the exploitation of the CVE as part of their attack vector
Pre-NVD Chatter	If a pre-NVD vulnerability has been talked about in 3 or more sources 5 or more times anywhere on the web; available for all CVEs
Published and Last Modified	Timestamp of when the CVE was published and updated in the NVD
Vulnerable Products	Common Platform Enumeration (CPE) data on the products to which this vulnerability definition applies

Table 1. A sample of data fields within Cisco Vulnerability Intelligence. This list is not exhaustive. For a full list, see full API Documentation.

Enrich Your Vulnerability Data

Cisco Vulnerability Intelligence's API lets organizations query and export actionable information from a multitude of detailed attributes for any CVE, including descriptions, publication dates, Common Vulnerability Scoring System (CVSS) data, available exploits, available fixes, if the vulnerability is exploitable by a remote code execution, list of vulnerable products, and much more. Also provided is the Cisco Security Risk Score and intel on predicted exploitability for each vulnerability—unique data points derived by Cisco Vulnerability Management's advanced data science.

Exploit Intel	Threat Intel
Metasploit	AlienVault OTX
Canvas Exploitation Framework	AlienVault Reputation
Github Exploit Feed – Cyentia Institute	Silobreaker Threat Intelligence
Exploit DB	Secureworks CTU
Black Hat Kits on rotation	Emerging Threats
Secureworks CTU	Reversing Labs
CISA Known Exploited Vulnerabilities	SANS Internet Storm Center
Contagio	X-Force Exchange
D2 Elliot	Cisco Talos Zero Days
Proofpoint	Cyentia Exploit Intelligence Service

Table 2. Exploit and threat intelligence feeds leveraged by Cisco Vulnerability Intelligence.

All CVEs within Cisco Vulnerability Intelligence are scored by Cisco and accompanied by a wealth of detailed attack and exploit information derived from a broad set of exploit and threat intelligence feeds, listed in Table 2.

With Cisco Vulnerability Intelligence, security and DevOps teams have unmatched breadth of CVE data at their fingertips.

Cisco Vulnerability Intelligence can be purchased standalone or as part of Cisco Vulnerability Management Premier. If you're interested in exploring how Cisco Vulnerability Intelligence can supercharge your VM program, request a demo today.