KENNA Security

Kenna.VI+

A Vulnerability Intel API to Enhance Your VM Workflows

KENNA.VI+ (Vulnerability Intel Plus) gives security teams access to the industry's richest consolidation of vulnerability intel via an API. Kenna.VI+ incorporates rich CVE data from more than 18 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).

World-Class CVE Enrichment for Security Alerts, Vulnerability Scans, and CI/CD Pipelines

Kenna.VI+ 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 a Kenna Risk Score and intel on predicted exploitability for each vulnerability—unique data points derived by Kenna's advanced data science.

Benefits

- **Enhance Your Security Research:** Query and export individual records to understand how attackers can exploit CVEs in the real world and inform your defense measures. A Postman library is available to streamline getting access to the data.
- **Enrich Your Vulnerability Data:** Overlay your existing data sources with Kenna's unique vulnerability intel to add additional context around CVEs.
- **Make Your VM Platform Smarter:** Integrate Kenna's vulnerability intelligence into any VM workflow and maximize the ROI of your existing VM solution deployment(s).
- **Built-In Data Science:** View Kenna Risk Score and predicted exploitability of a CVE—unique data points derived from Kenna's machine learning—for a greater level of vulnerability insight and prioritization.

Kenna Intelligence Feeds

EXPLOIT INTELLIGENCE:

- Canvas Exploitation Framework
- Contagio
- D2 Elliot
- Exploit DB
- Github Exploit Feed - Cyentia Institute
- Metasploit
- ReversingLabs
- Proofpoint
- Secureworks CTU
- Black Hat Kits on rotation (AlphaPack, Blackhole, Phoenix, more)

THREAT INTELLIGENCE:

- AlienVault OTX
- AlienVault Reputation
- Emerging Threats
- Exodus Intelligence
- ReversingLabs
- Sans Internet Storm Centre
- Secureworks CTU
- Silobreaker Threat Intelligence
- X-Force Exchange

Examples of Kenna.VI+ CVE Data	
Popular Target	If a vulnerability is trending across Kenna's customer base
Risk Score	Kenna Security unique risk score (1-100)
Remote Code Execution	If a CVE is capable of being exploited remotely
Predicted Exploitable	If Kenna predicts future exploits to develop that leverage a CVE
Active Internet Breach	If Kenna 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

Find out more about the robust vulnerability intelligence of Kenna.VI+ at
at **www.kennasecurity.com**

KENNA
Security
A part of Cisco.