**Now for the upcoming feature in my TIP, NLP assistant, i want the sites that uploads the daily suggested vulnerabilities so that i can integrate them into my project to warn people about them. Examples: CVE, CWE, CVSS Scores, ATT&CK mapping, Exploit info, Detection rules, Threat actor links, Real-world exploitation status, Mitigations**

Here are several high-quality, daily-updated **vulnerability intelligence sources** covering CVEs, CWE, CVSS scores, ATT&CK mappings, exploit data, real-world exploitation status, mitigation guidance, and more—perfect for integrating into your NLP assistant in your Threat Intelligence Platform (TIP):

**Trusted Daily Vulnerability Feeds & APIs**

**1. NVD – National Vulnerability Database (via NIST)**

* Provides **CVE feeds** in JSON format, including "recent" and "modified" daily files, as well as comprehensive JSON/CPE feeds [NVD](https://nvd.nist.gov/vuln/data-feeds?utm_source=chatgpt.com)[Dependency-Track](https://docs.dependencytrack.org/datasources/nvd/?utm_source=chatgpt.com).
* Offers a RESTful **CVE API (v2.0)**—updated in near real-time, supports filtering by publication or modification date, retrieving CVSS scores, CWEs, and other metadata [NVD](https://nvd.nist.gov/developers/vulnerabilities?utm_source=chatgpt.com).

**Integration Tip**: After an initial data load, periodically poll the API for CVEs published or modified since your last timestamp to stay up-to-date.

**2. CISA Known Exploited Vulnerabilities (KEV) Catalog**

* Contains vulnerabilities that are **actively exploited in the wild**, including CVE IDs, affected products, exploit status, and mitigation recommendations.
* Available in CSV, JSON, and schema formats [CISA](https://www.cisa.gov/known-exploited-vulnerabilities-catalog?utm_source=chatgpt.com).

**Integration Tip**: Consume the KEV catalog to prioritize high-impact vulnerabilities for rapid action or proactive alerts.

**3. CVE Details (cvedetails.com)**

* Offers an enhanced CVE database enriched with **advisories, exploits, EPSS/EPSS scores, open-source references**, and more.
* Supports **APIs, RSS feeds, email alerts, TAXII/STIX formats**—complete with CVSS scores and emerging CVE detection [CVE Details+1](https://www.cvedetails.com/?utm_source=chatgpt.com).

**Integration Tip**: Use their API endpoints (e.g., for ‘emerging CVEs’, vendor/product-specific queries, or score info) to bring richer context to your TIP.

**4. Vulners.com**

* Provides a structured vulnerability database with **millions of CVEs, exploits, articles, and intelligence**.
* Offers a reliable **Vulners REST API**, backed by a high uptime SLA and globally distributed infrastructure [Vulners](https://vulners.com/?utm_source=chatgpt.com).

**Integration Tip**: Use the Vulners API to fetch exploit-related data and threat actor insights.

**5. vFeed**

* A powerful aggregator that merges data from multiple standards—**CVE, CWE, CAPEC, ATT&CK, OVAL, CPE**—into a unified feed with rich metadata and mapping, including mitigations and attack patterns [vfeed.io](https://vfeed.io/standards/?utm_source=chatgpt.com).

**Integration Tip**: Ideal for cross-mapping CVEs to ATT&CK techniques, providing strong analytical capabilities in your TIP.

**6. EUVD – European Union Vulnerability Database**

* A newly launched EU-based vulnerability registry, complementing CVE, with EUVD identifiers and cross-references to CVEs.
* Active since mid-2025, it offers an expanding dataset from ENISA’s mandate under the NIS 2 Directive [Wikipedia](https://en.wikipedia.org/wiki/European_Union_Vulnerability_Database?utm_source=chatgpt.com).

**Integration Tip**: Consider incorporating as an alternative or supplementary regional feed, especially useful for EU-centric deployments.

**7. OpenCVE**

* Aggregates data from multiple CVE providers into a consolidated open-source interface, ensuring seamless updates and unified vulnerability information [OpenCVE](https://www.opencve.io/?utm_source=chatgpt.com).

**Integration Tip**: Excellent for lightweight, unified feeds without building multiple connectors.

**8. Sysdig Vulnerability Feeds**

* Synchronizes vulnerability feeds (e.g., NVD, Linux distros like Gentoo, Microsoft) **every 8 hours to daily**, ensuring freshness [docs.sysdig.com](https://docs.sysdig.com/en/sysdig-secure/vulnerability-feed/?utm_source=chatgpt.com).

**Integration Tip**: Useful for keeping your vulnerability repository refreshed across platforms.

**Quick Reference: Sources & Coverage**

| **Source** | **Key Coverage** | **Format / Access** |
| --- | --- | --- |
| **NVD (API & Feeds)** | CVE, CVSS, CWE, CPE, vendor comments, metadata | JSON feeds, REST API |
| **CISA KEV** | Exploited CVEs, mitigation guidance, real-world status | CSV, JSON |
| **CVE Details** | CVEs, exploits, EPSS, richer intelligence | APIs, RSS, TAXII/STIX, email |
| **Vulners** | CVE, exploits, articles, threat context | REST API |
| **vFeed** | CVE + CWE + CAPEC + ATT&CK + OVAL mappings | Aggregated feed |
| **EUVD** | EU-focused CVE mapping and identifiers | Public feeds (TBD) |
| **OpenCVE** | Multi-source CVE aggregation | Web UI/API |
| **Sysdig Feeds** | NVD + distro-specific vulnerability syncs | Regular feed updates |

**Integration Strategy for Your NLP Assistant**

1. **Primary CVE Source**: Use the **NVD API** for comprehensive, daily CVE ingestion including scoring and CWE data.
2. **Exploit & Real-World Prioritization**: Incorporate **CISA KEV** to flag actively exploited threats with urgency.
3. **Enriched Context**: Add **CVE Details** or **Vulners** APIs to supply enhanced data such as EPSS scores, advisories, and exploit references.
4. **Threat Framework Mapping**: Leverage **vFeed** for linking CVEs to ATT&CK, CAPEC, and mitigation controls.
5. **Regional/local insights**: Optionally include the **EUVD** if relevant for EU-based deployments.
6. **Redundancy and Monitoring**: Use **OpenCVE** and **Sysdig** as backups or additional sync mechanisms.