Mandiant

MANDIANT ADVANTAGE VULNERABILITY EXPLORER (MAVE) INTEGRATION

Developed By:	Mandiant
Latest Version:	1.22
Last Released:	August 2023
Key Contact:	**Support** (https://docs.mandiant.com/home/mandiant-support-cases)
Download:	**Mandiant.MAVE-lite.v1.22.zip** (https://dyzz9obi78pm5.cloudfront.net/app/image/id/6508d7c23533ca29137b8ae7/n/mandiantmave-litev122.zip) (md5: 487b8f4d23584210a26a433843b82db8)

MAVE Technical Acceleration

Mandiant Advantage Vulnerability Explorer (MAVE) is a proprietary python3 script that lets you interact directly with the Mandiant Advantage Threat Intelligence (MATI) **API** (https://docs.mandiant.com/home/mati-threat-intelligence-api-v4). You can correlate your Common Vulnerability & Exposures IDs (CVE-IDs) against the vulnerability intelligence it provides.

MAVE is considered a Technical Acceleration capability for customer use. It provides an example script to demonstrate features or example code of how to perform a task with the MATI API. With the distributed license, the Mandiant team that built this product will provide support and update as time permits.

MAVE background

MAVE was primarily built for customers to easily query multiple vulnerabilities at the same time, and to review those results as a "set" of information. MAVE supports the common use case for analysts seeking quick, ad hoc answers from the MATI API regarding the results of an internal vulnerability scan, for example.

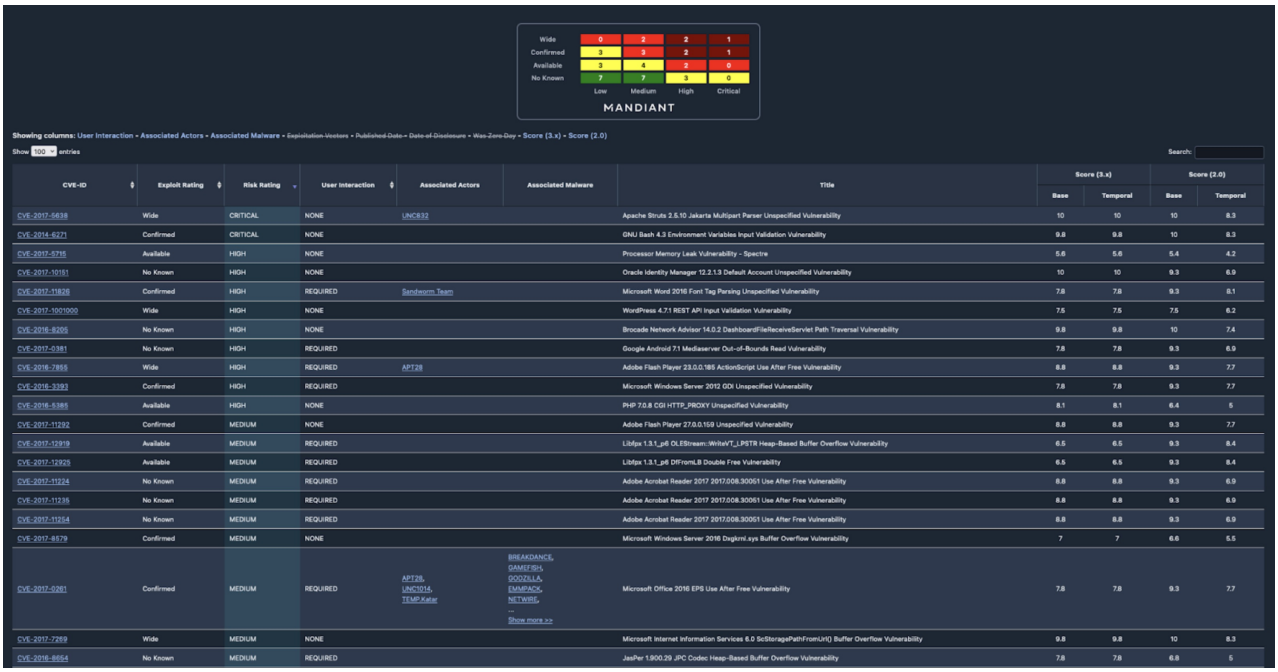
MAVE is a python3 script built to do the following:

1. Read a file from the command line
2. Extract the CVE-IDs from the file into a unique set
3. Query the MATI API for additional metadata on each vulnerability

MAVE outputs

If the API has CVE-ID matches, the results of the matches are populated into an HTML output file. You can optionally export the results into a CSV file for parsing and sorting larger datasets.

The HTML output file helps you prioritize your mitigation efforts by categorizing each vulnerability based on its Exploitation State (y-axis) and Risk Rating (x-axis). An intuitive chart that shows the number of vulnerabilities from the list that fall into each possible combination of these factors. Best practice is to focus first on vulnerabilities that have the highest values for both Exploit Rating and Risk Rating.



Up to ten columns can be displayed in the HTML output file. Columns can be added or removed as desired by selecting them from the **Showing columns** list.

Hyperlinks in the HTML output file let you quickly pivot to explore each vulnerability, associated threat actors, or malware families directly within the MATI platform.

- If a vulnerability has less than five linked actors or malware families, specific hyperlinks are provided for each actor/malware page within the MATI platform.
- If the vulnerability has more than five linked actors or malware families, only the hyperlink to the overarching vulnerability page is displayed. From there, you can select from the larger lists of actors and malware families.

The following video provides a detailed walkthrough of MAVE capabilities.

Release Notes

- **v1.22**
  - **New Features**:
    - Added support for rating_types filter for predicted, analyst, and unrated.
    - Updated the script processing limit to 50K CVE-IDs.
  - **Bug fix**: Resolved an issue to enable reuse of session connections.
- **v1.19**
  - **New feature**: Added CVE-IDs that have no API response into the log file (unenriched CVE-IDs).
  - **Bug fix**: Resolved an issue where a special character in the response CVE-ID title did not render correctly in the HTML output file.