

Forum:[Hack Forums](#)

Thread: [Vulnerability Parsing Utility](#)

ElmagoLoko - March 9, 2017, 5:16 pm

Vulnerator has been designed to assist U.S. Department of Defense (DoD) cybersecurity analysts with the daunting task of consolidating vulnerability data from the numerous sources that have been mandated:

The Assured Compliance Assessment Solution (ACAS)
Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
Security Content Automation Protocol (SCAP) content parsed via ACAS or the SCAP Compliance Checker (SCC)¹
Windows Automated Security Scanning Program (WASSP)

age Selector: A tab control that allows you to navigate amongst the various features of Vulnerator:
Reporting: The main feature of the application, this tab contains all of the controls related to parsing vulnerability files and creating human-readable reports from them. This tab is the main splash page for the application

Mitigations: The page containing the graphical interface for creating and maintaining reusable mitigations for ongoing vulnerabilities

Vulnerability Glance: This tab provides a quick insight into the results of the most recently parsed vulnerabilities. This tab contains additional reporting functionality surrounding IAVMs, and is currently under construction

Asset Contacts: Another feature currently in the development process, this is designed to allow users to quickly and efficiently build a listing of customers for each individual system as well as user-defined groups of systems. Once created, these lists will be able to be used to generate emails to contacts informing them of current vulnerabilities that fall under their area or responsibility

Reporting Options Pane: This is the main control hub of the application; it is within this pane that you will provide the parameters regarding the report(s) that you want to construct as well as the raw vulnerability files to be parsed. This area also contains the "Execute" file for vulnerability parsing

File Listing: A grid showing the current listing of files to be parsed, their type, and their current status

Window Controls: Similar to other Windows applications, these controls affect the positioning of the window (full screen, partial screen, minimized, and closed); take note that closing the window also exits the application

Flyout Command Buttons: These buttons will launch "flyout" windows that allow you to either view additional information about the program or customize the program to your liking, depending on which link is selected:

News: As of v6.1.1, Vulnerator now self reports on issues and releases posted on the project's GitHub site. Should you ever come across a bug or question the currency of the release you are using, this is a hub of information to which you can turn

About: Here, you can find information about the application such as the version you are running as well as contact details for the creator and links to pertinent sites

Theme: If you are going to look at a computer screen for any amount of time, it might as well be something you'd like to look at. Here, you have the ability to decide between a light or dark theme as well as an accent color of your choice

Status Bar: It is within this pane that you can check to verify the status of the activity you have performed – application progress and basic error reporting are noted here

File Counter: As the name implies, this is where you can quickly check to make sure that all of the

files you intend to parse are accounted for

QuickStart Guide

Now that you have familiarized yourself with the available resources (you did click the links, didn't you?), jump in to using the software!

Download the software from the Releases page

Note: Chances are, unless you are a coder or interested in seeing "under the hood", you want the compiled release (the download without the word "Source" in it)

Extract the entire folder from the "*.zip" file you just downloaded

Launch the "Vulnerator.exe" file from within the folder you just extracted

The executable has hidden files that it depends on to run – they are shipped with the application. If Vulnerator does not find these files in the directory it is in, it will yell at you, which will make you yell at me... and I don't like being yelled at.

Enjoy!

[Github](#)