Security Center 5.4 Vulnerability and Host Input for Firepower Management Center (6.0 +)

**File Summary:**

**Security Center Communications**

parameters.json

query\_vuln.py

sc\_connect.py.old.py

**Host Input (FMC) Communications**

<dir> InputPlugins

sf\_host\_input\_agent.pl

**Perl Modules for execution (must be installed)**

SFCheckPreReq.pm

SFHIclient.pm

SFHIlog.pm

SFHostInputAgent.pm

SFPkcs12.pm

**Prerequisites:**

This tool uses both python and perl to establish communications with Security Center and FMC to add vulnerability scan data (from Security Center) to the Host profile in FMC. In order for the tool to work properly the following requirements must be met

*\*\*Please be aware any prerequisites for the Host input client still exist and can be found @* [*https://www.cisco.com/c/en/us/td/docs/security/firepower/60/api/host-input/HostInputAPIGuide/Configuring-HostInputClient.html*](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/api/host-input/HostInputAPIGuide/Configuring-HostInputClient.html)

*If you were already using the older client prior you should already have met all those prerequisites.*

System:

Any POISX kernel based linux OS (tested and run in both Debian and CentOS)

Python:

Version 2.7.x is recommended

Requests

The request library is required for making REST calls to the Security Center. This library is built off python’s “urlib” to make REST based calls easier.

Requests can be installed by running either of the commands from the linux shell:

**pip install requests**

**easy\_install requests**

pySecurityCenter

Security Center 5.x has changed significantly vs the older 4.x and now uses RESTful methods to make calls. The pySecurityCenter wrapper makes developing against that API eaiser. To install the module you can run either of the commands from the linux shell:

**pip install pysecuritycenter**

**easy\_install pysecuritycenter**

**Using the script**

The script is fed by one user configurable file: “parameters.json.” These are the variables used to define the details of the Security Center and FMC that will be used.

Modify the file as follows:

{

"hostname" : "*<hostname or ip of security center>*",

"FMCHostname" : "*<hostname or ip of FMC>*",

"username" : "*<Security Center Username>*",

"password" : "*<Security Center Password>*",

"debug" : true,

"netrange" : "*<IP Range of hosts to add>*",

"addHosts" : true

}

It is recommended to leave the debug parameter true to help with troubleshooting if you were to have issues.

The addHosts parameter should only be set to “false” if you know for certain that the hosts for which you are adding vulnerability details already exist in the FMC.

Running the Script:

Before running the following command ensure that all prerequisites are met and the \*.pcks12 file from the FMC is in the same directory.

To run the tool simply execute:

**./query\_vuln.py**