pfSense Packages - Bug #14495

Snort does not contain DetectorFini() function

06/21/2023 04:06 PM - Jonathan Lee

Status:	Not a Bug	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Snort	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Affected Plus Version:**	23.05
Affected Version:	All	**Affected Architecture:**	SG-2100

Description

Detector cisco_content_group_dummy_detectors.lua: does not contain DetectorFini() function

I have been getting this error once and a while. I have posted to Netgate forum but no responses. This causes a fail open.

https://forum.netgate.com/topic/172958/detector-cisco_content_group_dummy_detectors-lua-does-not-contain-detectorfini-function

History

#1 - 06/21/2023 07:11 PM - Bill Meeks

This is not a bug. This is due to having incorrect user-supplied text rules for the current version of the OpenAppID detector stubs package. You are using an old and out-of-date user text rules package with OpenAppID. It is up to the OpenAppID function user to craft and configure the necessary text rules to work with the current OpenAppID rules stubs package from the Snort Vulnerability Research Team.

OpenAppID is NOT like the other rules at all. You can't simply enable it and have it work. User intervention is mandatory to craft and configure suitable text rules to stay in step with the rules stubs provided from Snort VRT. Those stubs frequently get updated by upstream.

As with everything the Snort binary does not like during startup, it will perform a FATAL ERROR exit and not continue startup. This behavior is by design in the Snort binary and cannot be changed short of rewriting the Snort binary. The "fail open" is how it is designed, unfortunately.

#2 - 06/21/2023 07:53 PM - Jonathan Lee

- File OpenDetectorDeveloperGuide.pdf added

I did not know this. Thanks for the reply. I have attached this for future reference should someone search for the same issue in the future. I just added this to the Netgate Forum also. Its SourceFire Open Source Detector Developers Guide. I got this pdf a couple years ago from someone.

#3 - 06/21/2023 09:57 PM - Marcos M

- Status changed from New to Not a Bug

Files

Screenshot 2023-06-21 at 9.05.43 AM.png	345 KB	06/21/2023	Jonathan Lee
OpenDetectorDeveloperGuide.pdf	433 KB	06/21/2023	Jonathan Lee