Known Issues List for AMSI and IPS EAP

Date: 12 February 2020

Enhanced Protection EAP with AMSI and IPS.

Endpoint

(See further for Server)

Core Agent: 2.6.0 BETA AMSI: 1.1.364 IPS (Network Threat Protection): 1.10.151

Issue	Details	Notes
[AMSI] Endpoints with AMSI may experience severe performance issues	This problem is not related to the Sophos implementation, but due to an issue in Windows. The issue occurs in rare circumstances. Disabling the setting does not fix the problem.	Currently the only solution is to manually deregister the AMSI Provider DLL as described in KBA 135127.
[Update] [IPS] IPS fails to attribute traffic to correct application due to packet modification	When certain applications such as NetBalancer are installed on the endpoint, IPS fails to correctly identify the source application of the malicious traffic. IPS still detects and blocks the malicious traffic, but fails to report the name of the application, nor can it block the application.	This issue has been fixed in the February 2020 EAP Update

Server

Issue	Details	Notes
[AMSI] AMSI missing on Server Core installations for 32-bit applications	When installing Windows Server 2016 and Windows Server 2019, in Server Core, native Microsoft AMSI support is missing for 32-bit applications.	As Powershell is the most important 32-bit application that should call AMSI, we recommend using AppLocker to disable this instance (for example using %windir%\SysWoW64\WindowsPowerShell*).

		Note that this does not mitigates all risks.