McAfee Host Intrusion Prevention Content 4803

Release Notes | 2013-03-12

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 4803)

New Windows Signatures

[New]Signature 2829: Block Packet Sniffer

Description:

- *This event indicates an attempt to install packet sniffing tools or capture network data using packet sniffing tools. Currently only few sniffing tools are supported.*
- *This signature is disabled by default.*

[New]Signature 2830: Block User Creation

Description:

- *This event indicates an attempt to create a new user on the system*
- *This signature is not supported on Windows Server 2008 and windows server 2008R2*
- *This signature is disabled by default*

[New]Signature 2831: Microsoft SharePoint Server JavaScript Elements Privilege Escalation

Description:

- *This event indicates an attempt to exploit a XSS vulnerability in the Microsoft SharePoint Server that could allow attackers to inject javascript code into a web page.*
- *This signature is set to level Medium by default.*

Updated Windows Signatures

[Updated]Signature 6013: Suspicious Function Invocation - CALL Not Found

Description:

- *The signature has been modified to reduce the false positives*

[Updated]Signature 532: Suspicious MSSQL Aux. Envelope - File Execution by MSSQL

Description:

- *The signature has been modified to reduce the false positives*

[Bugfix]: Added support for VMWARE9

[Bugfix]: Fix for compatibility issue with Endpoint Encryption for Files and Folders on HIPS7

How to Update

You need to check in the update package to the ePO Repository, and then send the updated information to the agents. Please refer to 'Updating' in Chapter 8 of 'Host Intrusion Prevention Product Guide'