McAfee Host Intrusion Prevention Content 5073

Release Notes | 2013-08-13

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 5073)

New Windows Signatures

***[New] Signature 2840*:** Microsoft Windows Media Format Video Decoder Remote Code Execution Vulnerability

Description:

- *This event indicates an attempt to exploit a vulnerability in Microsoft Media WMVCore.dll ActiveX Control that could allow attackers to execute code remotely.*
- *This signature is set to "HIGH" by default.*

***[New] Signature 6025*:** Timed Group Enabled / Expired

Description:

- *This event indicates the status of the Timed Group.*
- *This signature is enabled and the severity is set to Information by default.*
- *This signature requires HIPS 8.0 Patch 4 and above.*

***[New] Signature 6052*:** Generic Privilege Escalation Prevention

Description:

- *This event indicates a suspicious attempt to invoke a function with elevated privilege, a probable EoP attack.*
- *This signature is disabled by default.*
- *This signature requires HIPS 8.0 Patch 4 and above.*

***[New] Signature 6055*:** Exploitation using Windows Hot Patch Routine

Description:

- *This event indicates there was an attempt to exploit a vulnerability using LdrHotPatchRoutine to bypass Windows protection mechanism*
- *This signature is supported only on HIPS 8.0 and above, and only support 64bit Windows.*
- *This signature is set to "HIGH" by default.*

Bugfix and Updated Windows Signatures

[Bugfix]: SQL protection has been added for hot-fixes of SQL 2005 (SP4 CU1, SP4CU2 and SP4 CU3)**.**

[Updated] Signature 502*: MSSQL Core Shielding - File Execution*
Description:

- *The signature has been modified to reduce the False Positives.*

[Updated] Signature 515*: MSSQL Aux. Shielding - Service Reg. Modification*
Description:

- *The signature has been modified to reduce the False Positives.*

[Updated] Signature 523*: MSSQL Core Envelope - Registry Mod. by MSSQL*
Description:

- *The signature has been modified to reduce the False Positives.*

[Updated] Signature 556*: MSSQL SQL Shutdown Description:*
Description:

- *The signature has been modified to reduce the False Positives.*

[Updated] Signature 990*: Access Protection - New Startup Folder Program Creation*
Description:

- *The signature has been modified to reduce the False Positives.*

[Updated] Signature 1000*: Windows Agent Shielding - Service Access Description:*
Description:

- *The signature has been modified to reduce the False Positives.*

[Updated] Signature 1001*: Windows Agent Shielding - File Modification*
Description:

- *The signature has been modified to reduce the False Positives*

[Updated] Signature 1003*: Windows Agent Shielding - Process Access:*
Description:

- *The signature has been modified to reduce the False Positives.*

[Updated] Signature 1024*: Windows McAfee Agent Shielding - File Modification*
Description:

- *The signature has been modified to increase the coverage.*

[Updated] Signature 1281*: IIS6 Shielding - File Execution*
Description:

- *The signature has been modified to reduce the False Positives.*

***[Updated] Signature 2806**: Attempt to create a hardlink to a file*
Description:

The signature has been modified to reduce the False Positives.

***[Updated] Signature 3888**: Access Protection - Prevent Windows Process spoofing*
Description:

- *The signature has been modified to reduce the False Positives.*

***[Updated] Signature 3890**: Access Protection - Protect Internet Explorer favorites and settings*
Description:

- *The signature has been modified to reduce the False Positives.*

***[Updated] Signature 3897**: Access Protection - Protect cached files from password and email address stealers*
Description:

- *The signature has been modified to reduce the False Positives.*

***[Updated] Signature 6010**: Generic Application Hooking Protection*
Description:

- *The signature has been modified to reduce the False Positives.*

***[Updated] Signature 6011**: Generic Application Hooking Protection*
Description:

- *The signature has been modified to reduce the False Positives.*

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'