McAfee Host Intrusion Prevention Content 4739

Release Notes | 2013-02-12

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 4739)

New Windows Signatures

***[New]Signature 6044**: Vulnerability in DNSAPI Allow Remote Code Execution*

Description:

- *This event indicates an attempt to exploit vulnerability in DNSAPI remotely. This event is triggered when a malicious LLMNR message is received.*
- *This signature is set to level high by default.*

Updated Windows Signatures

***[Updated]Signature 2285**: Active Directory SPN Validation Vulnerability*

Description:

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

***[Updated]Signature 2821**: Access Protection - Prevent unknown processes to modify/patch or delete system drivers*

Description:

- *The signature has been modified to provide enhanced protection.*

***[Updated]Signature 2822**: ZeroAccess malware Infection*

Description:

- *The signature has been modified to provide enhanced protection.*

***[Updated]Signature 3891:** Access Protection - Prevent installation of new CLSIDs, APPIDs and TYPELIBs*

Description:

- *The signature has been modified to provide enhanced protection.*

***[Updated]Signature 6006:** Generic SQL Injection – IV*

Description:

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

Updated Solaris Signatures

[Updated]Signature 1008: *Solaris Agent Shielding - File Modification*

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'