McAfee Host Intrusion Prevention Content 5626

Release Notes | 2014-05-13

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 5626)

New Windows Signatures

[New]Signature 2851: *Microsoft SharePoint Server 2013 XSS Vulnerability*
Description:

- *This event indicates an attempt to exploit a XSS vulnerability in the Microsoft SharePoint Server 2013 that could allow attackers to inject javascript code into a web page (CVE-2014-1754).*
- *This signature is set to level Medium by default.*

[New]Signature 6058: *SSL Heartbleed Unencrypted Attack*
Description:

- *This event indicates receiving malformed SSL Heartbleed unencrypted attack packet.*
- *This signature is set to level High by default.*
- *Note: This signature requires HIP version 8.0 Patch 2 or later. Refer to KB article 51504 for details about supported platforms*

Updated Windows Signatures

BugFix*: Signature description for HIPS signatures has been modified to remove excessive spacing*

[Updated]Signature 413*: Suspicious Double File Extension Execution*
Description:

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

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

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

***[Updated]Signature 3754**: Illegal Execution in winword.exe*
Description:

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

***[Updated]Signature 3905**: Access Protection - Prevent all programs from running files from the Temp folder*
Description:

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

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

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

***[Updated]Signature 6014**: Suspicious Function Invocation - Return Address Not Readable*
Description:

- *This signature has been modified to reduce the false positives.*
- *Signature support for 32 bit process on 64 bit platforms is suspended.*

***[Updated]Signature 6049**: Suspicious Function Invocation - No Module*
Description:

- *This 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'