McAfee Host Intrusion Prevention Content 5209

Release Notes | 2013-11-12

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 5209)

New Windows Signatures

[New] Signature 2842: Exploitation using Library load from UNC Path

Description:

- *This event indicates library load from UNC path which allows attacker to exploit remote code execution vulnerability.*
- *This signature is disabled by default*

[New] Signature 2844: Microsoft Word WordPerect5 Converter Module Buffer Overflow Vulnerability

Description:

- *This event indicates an attempt to exploit a vulnerability exists in Microsoft Word that loads WordPerfect5 converter module which contains multiple buffer overflow vulnerabilities.*
- *This signature is disabled by default.*

[New] Signature 2846: InformationCardSigninHelper ActiveX Control Vulnerability

Description:

- *This event indicates an attempt to exploit a vulnerability in Microsoft InformationCardSigninHelper ActiveX Control in ICARDIE.DLL that could allow attackers to execute code remotely*
- *This signature is set at level 'High' by default*

***[New] Signature 6666*:** Generic Java Sandbox Escape Exploit Detected

Description:

- *This event indicates an attempt to exploit a sandbox bypass vulnerability that exists in Oracle Java Applets.*
- *This signature is set at level 'Informational' and in later releases planned to be set at higher levels.*

***[New] Signature* 8000**: Remote Code Execution Attack

Description:

- *This event indicates a remote code execution attack*
- *This signature is set at level 'Informational' and in later releases planned to be set at higher levels.*

***[New] Signature* 8001**: Suspicious Remote Code Execution Attack

Description:

- *This event indicates a suspicious remote code execution attack.*
- *This signature is set at level 'Informational' and in later releases planned to be set at higher levels.*

***[New] Signature 8002*:** Possible Remote Code Execution Attack

Description:

- *This event indicates a possible remote code execution attack*
- *This signature is set at level 'Informational' by default.*

Updated Windows Signatures

***[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 reduce the false positives*

***[Updated]Signature 2805**: Opening Email client as Administrator*

Description:

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

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

Description:

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

***[Updated]Signature 3922**: Illegal Execution in Microsoft Excel*

Description:

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

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

Description:

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

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

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'