



McAfee Host Intrusion Prevention Content 4110

Release Notes | 2012-01-10

Below is the new/updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 4110)

New Windows Signatures

[New] Signature 2297: Access Protection - Prevent common programs from running files from the Temp folder

Description:

- This signature prevents common programs from executing files from the temp folder.
- *This signature is disabled by default.*

[New] Signature 2786: IIS 6.0 Denial of Service Vulnerability

Description:

- This event indicates an attempt to exploit a Denial of Service vulnerability that may result in information disclosure.
- *This signature is set to informational level by default.*
- *Note: This signature does not provide protection on Windows Server 2003(x64) with HIPS 7.0*

Updated Windows Signatures

[Updated] Signature 3906: Access Protection - Prevent programs registering to auto run

- *The signature has been modified to enhance the protection by providing better coverage and reducing the false positives.*

[Updated]Signature 3904: Access Protection - Protect network settings

- *The signature has been modified to enhance the protection by providing the better coverage.*

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

- *The signature has been modified to enhance the protection.*

[Updated]Signature 850: Change of Service Executable

- *The signature has been modified to enhance the protection.*

[Updated]Signature 345: Registry Access Limitations Lifted

- *The signature has been modified to enhance the protection.*

[Updated]Signature 987: Event Log File or Related File Modification

- *The signature has been modified to enhance the protection.*

[Updated]Signature 3870: VMware Workstation Shielding - Service Modification

- *The signature has been modified to enhance the protection by providing better coverage and reducing the false positives.*

[Updated]Signature 911: Event Log File or Related File Deleted

- *The signature has been modified to enhance the protection.*

[Updated]Signature 6033: Shortcut Icon Loading Vulnerability

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

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

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

[Updated]Signature 907: PW Dump Tool Activation

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

[Updated]Signature 2779: TDSS Rootkit Infection

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

[Updated] Bug fix: Content support for SQL version 10.0.4064.0

- *The content has been modified to support the SQL version 10.0.4064.0*

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'