McAfee Host Intrusion Prevention Content 6952

Release Notes | 2016-05-10

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 6952)

New Windows Signature

***[New] Signature 6073**: Execution Policy Bypass in Powershell*
(BZ #1130807)

- *This event indicates that Execution Policy of Windows powershell has been set to bypass.*
- *Signature is disabled by default.*
- *The signature is supported only on HIPS 8 and above platforms.*

Note: Customers can change the level of this signature as per their requirement.

***[New] Signature 6074**: PlugX Malware infection*

- *This event indicates an attempt by the PlugX malware to infect the system.*
- *Signature is disabled by default.*
- *The signature is supported only on HIPS 8 and above platforms.*

Note: Customers can change the level of this signature as per their requirement.

Updated Windows Signatures

***[Updated] Signature 3892**: Access Protection - Prevent termination of McAfee processes*
(BZ #1131642)
Description:

- *This signature modified to reduce the false positives*

***[Updated] Signature 3898**: Access Protection - Prevent modification of McAfee files and settings*
(BZ #1131642)
Description:

- *This signature modified to reduce the false positives*

***[BugFix]**: HIPS Startup IPS Protection rules are modified to reduce the false positives*

(BZ #1129321)

Existing coverage for New Vulnerabilities

Coverage by GBOP: *HIP GBOP Signatures 428, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:*

- *CVE-2016-0126*
- *CVE-2016-0178*
- *CVE-2016-0183*

Coverage by GBOP: *HIP GBOP Signatures 428, 1145, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:*

- *CVE-2016-0185*

Coverage by GBOP: *HIP GBOP Signatures 428, 1146, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:*

- *CVE-2016-0169*
- *CVE-2016-0187*
- *CVE-2016-0189*
- *CVE-2016-0192 (applicable only for Internet Explorer browser)*

Coverage by GBOP: *HIP GBOP Signatures 428, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:*

- *CVE-2016-0140*

Coverage by GPEP: *HIP Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:*

- *CVE-2016-0170*
- *CVE-2016-0171*
- *CVE-2016-0172*
- *CVE-2016-0173*
- *CVE-2016-0174*
- *CVE-2016-0175*
- *CVE-2016-0176*
- *CVE-2016-0179*
- *CVE-2016-0180*
- *CVE-2016-0196*

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’