McAfee Host Intrusion Prevention Content 7007

Release Notes | 2016-06-14

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 7007)

New Windows Signature

***[New] Signature 6075**: Remote script execution by core windows utility*

- *This event indicates an attempt by core windows utility to execute script from remote location.*
- *Signature is set level Low by default.*
- *The signature is supported only on HIPS 8 and above platforms.*
- *The signature is not supported on 64 bit processes.*
- *The signature is not supported on Endpoint Security Threat Prevention*

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

Updated Windows Signatures

***[Updated] Signature 6015**: Suspicious Function Invocation - Target Address Mismatch Description:*

- *This signature modified to reduce the false positives*

***[Updated]:** HIPS Content has been modified to support the new Intel Certificate signer*

***[Updated]:** Trusted application list has been modified to support the new Intel Certificate Signer.*

***[BugFix]**: Adobe Flash Player Plugin (32 bit process) for Mozilla Firefox browser is added into the default application protection list to improve the GBOP coverage*

Existing coverage for New Vulnerabilities

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

- *CVE-2016-0199*
- *CVE-2016-0200*
- *CVE-2016-3205*
- *CVE-2016-3206*
- *CVE-2016-3207*
- *CVE-2016-3210*

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

- *CVE-2016-3233*
- *CVE-2016-3234*

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

- *CVE-2016-0025*
- *CVE-2016-3216*
- *CVE-2016-3227*

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

- *CVE-2016-3218*
- *CVE-2016-3220*
- *CVE-2016-3221*

Coverage by other Existing HIP Signatures:

HIP Signature 3906 is expected to cover the below vulnerability:

- *CVE-2016-3211*

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'