McAfee Host Intrusion Prevention Content 7364

Release Notes | 2016-11-15

Below is the updated signature information for the McAfee Host Intrusion Prevention 8.0 content (version 7364)

Note: The Endpoint Security Exploit Prevention content version is 10.2.0.7364

New Windows Signatures

***Signature 6078**: Mimikatz usage*

Description:

- *This event indicates the presence of mimikatz tool on the system*
- *This signature is set to level Medium by default*
- *This is applicable for both 32-bit and 64-bit Windows Powershell processes*

Note: This signature is also applicable on Endpoint Security Threat Prevention

***Signature 6079**: Suspicious LSASS Access Detected*

Description:

- *This event indicates a suspicious attempt to access LSASS process*
- *This signature is disabled by default*

Note: The signature is not supported on Endpoint Security Threat Prevention.

***Signature 6080**: Mimikatz malware execution*

Description:

- *This event indicates a suspicious attempt to execute Mimikatz malware*
- *This signature is set to level High by default*

Note: The signature is not supported on Endpoint Security Threat Prevention.

Updated Windows Signatures

***[Updated] Signature 6070**: Hidden Powershell Detected*

Description:

- *This signature is modified to support 64 bit Windows Powershell process*
- *Default signature level is modified to Informational from Disabled*

***[Updated] Signature 6073**: Execution Policy Bypass in Powershell*

Description:

- *This signature is modified to support 64 bit Windows Powershell process*
- *Default signature level is modified to Informational from Disabled*

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

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

Other Changes

Inclusion of Host IPS 8.0 Hotfix 1153407

This content update also applies a Host IPS hotfix 1153407 on the client systems running Host IPS 8.0 Patch 5, Patch 6 or Patch 7 only. Successful installation of hotfix displays a different client version depending on which patch version is installed as indicated below:

- *Patch 7: 8.0.0.3800*
- *Patch 6: 8.0.0.3500*
- *Patch 5: 8.0.0.3250*

Refer below KB for more details on this hotfix.

https://kc.mcafee.com/corporate/index?page=content&id=KB87658

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-2016-7195*
- *CVE-2016-7196*
- *CVE-2016-7205*
- *CVE-2016-7241*

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

- *CVE-2016-7213*
- *CVE-2016-7228*
- *CVE-2016-7229*
- *CVE-2016-7231*

- *CVE-2016-7236*

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

- *CVE-2016-7212*
- *CVE-2016-7230*
- *CVE-2016-7232*
- *CVE-2016-7233*
- *CVE-2016-7234*
- *CVE-2016-7235*

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

- *CVE-2016-0026*
- *CVE-2016-3332*
- *CVE-2016-3333*
- *CVE-2016-3334*
- *CVE-2016-3335*
- *CVE-2016-3338*
- *CVE-2016-3340*
- *CVE-2016-3342*
- *CVE-2016-3343*
- *CVE-2016-7184*
- *CVE-2016-7215*
- *CVE-2016-7224*
- *CVE-2016-7226*
- *CVE-2016-7246*
- *CVE-2016-7255*

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'