



McAfee Host Intrusion Prevention Content 7440

Release Notes | 2016-12-13

Below is the updated signature information for the McAfee Host Intrusion Prevention 8.0 content (version 7440)

Note: The Endpoint Security Exploit Prevention content version is 10.5.0.7440

New Windows Signatures

Signature 6081: Powershell Command Restriction - NoProfile

Description:

- This event indicates an attempt to execute powershell with NoProfile parameter
- This signature is Disabled by default
- This is applicable for both 32-bit and 64-bit Windows Powershell processes

Note: Minimum Endpoint Security Product version required to support this signature is 10.5

Signature 6082: Powershell Command Restriction - ExecutionPolicy Unrestricted

Description:

- This event indicates an attempt to execute powershell with ExecutionPolicy Unrestricted parameter
- This signature is Disabled by default
- This is applicable for both 32-bit and 64-bit Windows Powershell processes

Note: Minimum Endpoint Security Product version required to support this signature is 10.5

Signature 6083: Powershell Command Restriction - NonInteractive

Description:

- This event indicates an attempt to execute powershell with NonInteractive parameter
- This signature is Disabled by default
- This is applicable for both 32-bit and 64-bit Windows Powershell processes

Note: Minimum Endpoint Security Product version required to support this signature is 10.5

Signature 6084: Powershell Command Restriction - NoLogo

Description:

- This event indicates an attempt to execute powershell with NoLogo parameter
- This signature is Disabled by default

- This is applicable for both 32-bit and 64-bit Windows Powershell processes

Note: Minimum Endpoint Security Product version required to support this signature is 10.5

Signature 6085: Powershell Command Restriction - File

Description:

- This event indicates an attempt to execute powershell with File parameter
- This signature is Disabled by default
- This is applicable for both 32-bit and 64-bit Windows Powershell processes

Note: Minimum Endpoint Security Product version required to support this signature is 10.5

Signature 6086: Powershell Command Restriction - Command

Description:

- This event indicates an attempt to execute powershell with Command parameter
- This signature is Disabled by default
- This is applicable for both 32-bit and 64-bit Windows Powershell processes

Note: Minimum Endpoint Security Product version required to support this signature is 10.5

Signature 6087: Powershell Command Restriction - EncodedCommand

Description:

- This event indicates an attempt to execute powershell with EncodedCommand parameter
- This signature is Disabled by default
- This is applicable for both 32-bit and 64-bit Windows Powershell processes

Note: Minimum Endpoint Security Product version required to support this signature is 10.5

Updated Windows Signatures

[Updated] Signature 6070: Hidden Powershell Detected

Description:

- This signature has been fine tuned to improve performance

[Updated] Signature 6073: Execution Policy Bypass in Powershell

Description:

- This signature has been fine tuned to improve performance

[Updated] Signature 6078: Mimikatz usage

Description:

- This signature has been fine tuned to improve performance

[Updated]: HIPS Content Start-up IPS protection has been modified to improve the protection

[BugFix]: HIPS Content has been modified to fix the NIPS Signature loading issue observed for Russian Locale

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-2016-7202
- CVE-2016-7272
- CVE-2016-7279
- CVE-2016-7283
- CVE-2016-7284
- CVE-2016-7293

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

- CVE-2016-7257
- CVE-2016-7264
- CVE-2016-7265
- CVE-2016-7277

Coverage by GBOP: HIP GBOP Signatures 428, 1146, 3922, 6012, 6013 and 6014 are expected to cover the below vulnerabilities:

- CVE-2016-7278

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

- CVE-2016-7268
- CVE-2016-7276
- CVE-2016-7289

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

- CVE-2016-7219
- CVE-2016-7259
- CVE-2016-7260
- CVE-2016-7274

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'