



## McAfee Host Intrusion Prevention Content 7245

### Release Notes | 2016-09-20

Below is the updated signature information for the McAfee Host Intrusion Prevention 8.0 content (version 7245)

**Note:** The Endpoint Security Exploit Prevention content version is 10.2.0.7245

---

#### New Windows Signatures

**Signature 6076:** Microsoft Windows Media Center MCL Vulnerability  
(CVE-2015-2509) (BZ #1145939)

Description:

- This signature prevents execution of a remote file by Windows media center.
  - This signature is disabled by default.
- 

#### Updated Windows Signatures

**[Updated] Signature 1000:** Windows Agent Shielding - Service Access  
(BZ #1148853)

Description:

- This signature is modified to reduce the false positives

**[Updated] Signature 1001:** Windows Agent Shielding - File Modification  
(BZ #1148853)

Description:

- This signature is modified to reduce the false positives

**[Updated] Signature 1002:** Windows Agent Shielding - Registry Access  
(BZ #1148853)

Description:

- This signature is modified to reduce the false positives

**[Updated] Signature 1003:** *Windows Agent Shielding - Process Access*  
(BZ #1148853)

Description:

- *This signature is modified to reduce the false positives*

**[Updated] Signature 1020:** *Windows Agent Shielding - File Access*  
(BZ #1148853)

Description:

- *This signature is modified to reduce the false positives*

**[Updated] Signature 6067:** *Self Protection – Critical Registry Access*  
(BZ #1148853)

Description:

- *This signature is modified to reduce the false positives*

**[Updated] Signature 6024:** *TrustedSource Remote IP address blocked*  
(BZ #1150044)

Description:

- *This signature's description has been changed for more clarity.*

**[Updated] Signature 6025:** *Timed Group Enabled / Expired*  
(BZ #1150044)

Description:

- *This signature's description has been changed for more clarity.*

**[Updated] Signature 6065:** *Policy Load Status*  
(BZ #1150044)

Description:

- *This signature's description has been changed for more clarity.*

**[Bug Fix]** *Host IPS content install script has been modified for Host IPS 8.0 Patch 5 systems. (BZ #1157088)*

---

## **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-2016-3297
- CVE-2016-3324
- CVE-2016-3375
- CVE-2016-3376

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

- CVE-2016-3358
- CVE-2016-3359
- CVE-2016-3362
- CVE-2016-3363
- CVE-2016-3365

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

- CVE-2016-3357
- CVE-2016-3360
- CVE-2016-3368

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

- CVE-2016-3348
- CVE-2016-3355

## 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'