



## McAfee Host Intrusion Prevention Content 7304

### Release Notes | 2016-10-11

Below is the updated signature information for the McAfee Host Intrusion Prevention 8.0 content (version 7304)

**Note:** The Endpoint Security Exploit Prevention content version is 10.2.0.7304

---

#### New Windows Signatures

**Signature 6077:** Microsoft Visio DLL Hijacking Vulnerability  
(CVE-2016-3364)

Description:

- This event indicates an attempt to exploit a vulnerability in Visio 2016 which leads to DLL Hijacking
- This signature is disabled by default.

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

---

#### Updated Windows Signatures

**[Updated] Signature 3872:** VMWare Workstation Shielding - File Modification  
(BZ #1159983)

Description:

- This signature is modified to reduce the false positives

**[Updated] Signature 6066:** Illegal Execution - Writable Memory II  
(BZ #1157695)

Description:

- This signature is modified to reduce the false positives
-

## 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-2016-3382
- CVE-2016-3383
- CVE-2016-3385

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

- CVE-2016-7193

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

- CVE-2016-0026
- CVE-2016-0070
- CVE-2016-3266
- CVE-2016-3270
- CVE-2016-3332
- CVE-2016-3333
- CVE-2016-3334
- CVE-2016-3335
- CVE-2016-3338
- CVE-2016-3340
- CVE-2016-3341
- CVE-2016-3342
- CVE-2016-3343
- CVE-2016-3376

- *CVE-2016-7182*
- *CVE-2016-7184*
- *CVE-2016-7185*
- *CVE-2016-7191*

## **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'