



## McAfee Host Intrusion Prevention Content 6015

### Release Notes | 2014-10-16

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 6015)

---

#### New Non-Windows Signatures

**[New]Signature 1776:** *Apache Shellshock Bash Environment Variable Code Injection Attack (CVE-2014-6271)*

*Description:*

- *This event indicates an attempt of injecting code to the Apache web server CGI remotely, and result in arbitrary code execution.*
- *This signature is set to level Low by default*

*Note:* *This signature is supported only on Solaris platforms*

*This Signature covers only one of the Exploitation method of Apache web server CGI injection for Shellshock vulnerability*

*It is advised that the level of this signature can be adjusted as needed.*

**[New]Signature 3342:** *Apache Shellshock Bash Environment Variable Code Injection Attack (CVE-2014-6271)*

*Description:*

- *This event indicates an attempt of injecting code to the Apache web server CGI remotely, and result in arbitrary code execution.*
- *This signature is set to level Low by default*

*Note:* *This signature is supported only on Red Hat flavors of Linux.*

*This Signature covers only one of the Exploitation method of Apache web server CGI injection for Shellshock vulnerability*

*It is advised that the level of this signature can be adjusted as needed.*

#### Updated Windows Signatures

**[Updated]Signature 2787:** *W32/Yunsip Infection (BZ #1009020)*

*Description:*

- *This signature has been modified to reduce the false positives.*

**[Updated]Signature 3922:** *Illegal Execution in Microsoft Excel (BZ #1006449)*

Description:

- *This signature has been modified to reduce the false positives.*

**[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.*

---

### **Existing coverage for New Vulnerabilities**

**Coverage by GBOP:** *HIP GBOP is expected to cover the below vulnerabilities:*

- *CVE-2014-2812*
- *CVE-2014-4125*
- *CVE-2014-4126*
- *CVE-2014-4127*
- *CVE-2014-4128*
- *CVE-2014-4129*
- *CVE-2014-4130*
- *CVE-2014-4131*
- *CVE-2014-4132*
- *CVE-2014-4133*
- *CVE-2014-4134*
- *CVE-2014-4135*
- *CVE-2014-4136*
- *CVE-2014-4137*
- *CVE-2014-4138*
- *CVE-2014-4139*
- *CVE-2014-4141*
- *CVE-2014-4143*
- *CVE-2014-4146*
- *CVE-2014-4147*
- *CVE-2014-4118*
- *CVE-2014-4121*
- *CVE-2014-4117*

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

- *CVE-2014-4115*
- *CVE-2014-4113*
- *CVE-2014-4148*

## **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'