McAfee Host Intrusion Prevention Content 6785

Release Notes | 2015-12-08

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 6785)

Updated Windows Signatures

***[Updated]Signature 1002**: Windows Agent Shielding - Registry Access*
Description:

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

***[Updated]Signature 1205**: IIS Envelope - File Access by IIS Web User*
Description:

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

***[Updated]Signature 1225**: IIS Envelope - File Access by IIS Process*
Description:

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

***[Updated]Signature 1226**: IIS Envelope - File Modification by IIS Process*
Description:

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

***[Updated]Signature 1260**: IIS6 Envelope - File Access by IIS Process*
Description:

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

***[Updated]Signature 1261**: IIS6 Envelope - File Access by IIS Web User*
Description:

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

***[Updated]Signature 1264**: IIS6 Envelope - File Modification by IIS Process*
Description:

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

***[Updated]Signature 2787**: W32/Yunsip Infection*

Description:

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

***[Updated]Signature 6010**: Generic Application Hooking Protection*

Description:

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

***[Updated]Signature 6011**: Generic Application Invocation Protection*

Description:

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

***[Updated]Signature 6067**: Self Protection – Critical Registry Access*

Description:

- *This signature name and description has been changed for more clarity*

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-2015-6083*
- *CVE-2015-6134*
- *CVE-2015-6136*
- *CVE-2015-6140*
- *CVE-2015-6141*
- *CVE-2015-6142*
- *CVE-2015-6143*
- *CVE-2015-6145*
- *CVE-2015-6146*
- *CVE-2015-6147*
- *CVE-2015-6148*
- *CVE-2015-6149*
- *CVE-2015-6150*
- *CVE-2015-6151*
- *CVE-2015-6152*
- *CVE-2015-6153*
- *CVE-2015-6154*
- *CVE-2015-6155*
- *CVE-2015-6156*
- *CVE-2015-6158*
- *CVE-2015-6159*
- *CVE-2015-6160*

- *CVE-2015-6162*

HIP GBOP Signatures 428, 1139, 1140, 6012, 6013 and 6014 are expected to cover the below vulnerabilities

- CVE-2015-6106
- CVE-2015-6107
- CVE-2015-6108
- CVE-2015-6124
- CVE-2015-6125
- CVE-2015-6130
- CVE-2015-6136
- CVE-2015-6140
- CVE-2015-6142
- CVE-2015-6148
- CVE-2015-6151
- CVE-2015-6153
- CVE-2015-6154
- CVE-2015-6155
- CVE-2015-6158
- CVE-2015-6159
- CVE-2015-6166
- CVE-2015-6168
- CVE-2015-6172

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

- *CVE-*2015-*6040*
- CVE-2015-6118
- CVE-2015-6122
- CVE-2015-6177
-

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

- *CVE-2015-6126*
- *CVE-2015-6171*
- *CVE-2015-6173*
- *CVE-2015-6174*
- *CVE-2015-6175*

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’