



McAfee Host Intrusion Prevention Content 6821

Release Notes | 2016-01-12

Below is the updated signature information for the McAfee Host Intrusion Prevention 7.0/8.0 content (version 6821)

Updated Windows Signatures

[Updated]Signature 1000: Windows Agent Shielding - Service Access

Description:

- This signature has been modified to reduce the false positives

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

Description:

- This signature has been modified to reduce the false positives

[Updated]Signature 1003: Windows Agent Shielding - Process Access

Description:

- This signature has been modified to reduce the false positives

[Updated]Signature 2787: W32/Yunsip Infection

Description:

- This signature has been modified to fix an internal logging issue

[Updated]Signature 6500: SSH Version 2 Brute Force

(BZ 1106781)

Description:

- This signature has been modified to fix the intermittent BSOD issue with HIPS 8 Patch 6 platforms

Existing coverage for New Vulnerabilities

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

- CVE-2016-0002

- CVE-2016-0003
- CVE-2016-0010
- CVE-2016-0012
- CVE-2016-0015
- CVE-2016-0024
- CVE-2016-0034
- CVE-2016-0035

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

- CVE-2016-0009

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'