



2006-SEP-12

McAfee Host Intrusion Prevention 6.0 Content Release Notes

Below are the updates from the last release for McAfee Host Intrusion Prevention 6.0 content. The content build number is 610 (previous RTW: 567).

New/Updated Signatures

- (New) Sig 3762 "IE SourceURL NULL Vulnerability" (CVE-2006-3427)
- (New) Sig 3766/3767 "Windows Server Service Buffer Overflow Vulnerability" (CVE-2006-3439)
- (New) Sig 3769 "Windows Metafile Denial of Service Vulnerability" (CVE-2006-4071)
- (New) Sig 3771 "Microsoft Indexing Service Vulnerability" (CVE-2006-0032)
- (New) Sig 3764 "Illegal Execution in services.exe" (CVE-2006-3439) ^{*1}
- (New) Sig 3765 "Illegal Execution in svchost.exe" (CVE-2006-3439) ^{*1}
- (Updated) Sig 3737 "COM Object Instantiation Memory Corruption Vulnerability" (CVE-2006-3638)
- (Updated) Sig 3754 "Illegal Execution in winword.exe" (formerly named "MS Word Malformed Object Pointer Vulnerability") ^{*2}
- (Updated) Sig 3759 "MHTML Parsing Vulnerability" ^{*3}
- (Updated) Sig 1000, 1001, 1002, 1020 ^{*4}
- (Updated) Sig 3763 "Windows Kernel Elevation of Privilege Vulnerability" ^{*5}
- (Updated) Sig 3760 "Internet Explorer FTP Command Injection Vulnerability" ^{*6}

^{*1} Sig 3764 and 3765 were released in mid-August to mitigate MS06-040 exploits found after August content release. Now we have Kevlar signature 3766 and 3767 which can detect more attacks with a lower chance of false positives.

^{*2} Sig 3754 was created to address "MS Word Malformed Object Pointer Vulnerability" first but later it was found that it can block a 0day exploit for "MS Word Malformed String Vulnerability (CVE-2006-4534). Thus, the name has been changed accordingly.

^{*3} Sig 3759 now covers Outlook Express

^{*4} Firesvc.exe (part of Host Intrusion Prevention) is now excluded from agent self protection signatures (Sig 1000, 1001, 1002, 1020).

^{*5} Severity level is changed from high to medium.

^{*6} Signature now covers Windows NT

Updates on Trusted Applications

(none)

Updates on Application Protection Rules

(none)

How to Update

You need to check in the update package to the ePO Repository, then send the updated information to the agents. Please refer to 'Updating' in Chapter 8 of 'Host Intrusion Prevention 6.0 Product Guide'