

## McAfee Host Intrusion Prevention 6.1 Content Release Notes | 2007-05-08

Below are the updates from the last release for McAfee Host Intrusion Prevention 6.1 content. The content build number is 1104 (previous RTW: 1090).

---

### New/Updated Windows Signatures

- [new] Sig 3825 "CAPICOM.DLL Improper Arguments Vulnerability" (CVE-2007-0940)
- [new] Sig 3833 "Vulnerability in Research in Motion ActiveX control" (no-CVE-number)
- [new] Sig 3834 "Vulnerability in mdsauth ActiveX control" (CVE-2007-2221)
- [new] Sig 3835 "COM Object Instantiation Memory Corruption Vulnerability (5)" (CVE-2007-0942)
- [new] Sig 3841 "Akamai Download Manager ActiveX Stack Buffer Overflow Vulnerability" (CVE-2007-1891, CVE-2007-1892) <sup>\*1</sup>
- [new] Sig 3843 "Internet Explorer CSS Memory Corruption Vulnerability" (CVE-2007-0945) <sup>\*2</sup>
- [new] Sig 3844 "Microsoft Exchange DoS Vulnerability" (CVE-2007-0039) <sup>\*3</sup>

*\*1 – Disabled by default. Vulnerability CVE-2007-1891 affects Akamai Download Manager newer than 2.0.4.4 and older than 2.2.1.0. Vulnerability CVE-2007-1892 affects all versions prior to 2.2.1.0. Customers using these versions are advised to turn on the signature or to install version 2.2.1.0.*

*\*2 – Disabled by default. Customers who need the protection are advised to turn it on.*

*\*3 – Disabled by default. Customers who need the protection are advised to turn it on. Turning on this signature will cause loss of functionalities such as sending and exchanging information related to calendars and scheduling.*

---

### Updates on Application Protection Rules for Windows

- [new] tcpsvcs.exe – Microsoft Windows Networking Services (DHCPService, BINLSVC, SimpTcp, LPDSVC)
- [new] mnmsrvc.exe - NetMeeting Remote Desktop Sharing

---

## New/Updated Solaris Signatures

- [new] Sig 1761 "Sun Solaris Mozilla Network Security Services Buffer Overflow Vulnerabilities" (CVE-2007-0008, CVE-2007-0009)
- [new] Sig 1762 "Sun Solaris Adobe Reader Remote Code Execution Vulnerability" (CVE-2006-5857)

---

## New/Updated Linux Signatures

- [new] Sig 3055 "Linux - Vulnerability in sharutils could allow Elevation of Privileges" (CVE-2005-0990)
- [new] Sig 3056 "Linux - Vulnerability in mysql could allow Elevation of Privileges via symlink attacks" (CVE-2005-0711)
- [new] Sig 3057 "Linux - Vulnerability in vim could allow Elevation of Privileges" (CVE-2005-0069)

### 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 6.1 Product Guide'