McAfee® Labs
Security Threat Advisory

McAfee

May 28, 2010

MTIS10-102

Executive Summary

Since the last McAfee® Labs Security Advisory (May 28), the following noteworthy events have taken place:

- McAfee product coverage has been updated for a vulnerability in Apple's Safari.
- McAfee product coverage has been updated for vulnerabilities in Adobe's ColdFusion.
- McAfee product coverage has been updated for a vulnerability in HP's OpenView Network Node Manager.
- McAfee product coverage has been updated for a vulnerability in Microsoft's Windows Canonical Display Driver.
- McAfee product coverage has been updated for a vulnerability in Adobe's Photoshop.

McAfee product coverage for these events:

McAfee Product Coverage Updates *

Threat	Advisory	Impor-tance	DAT	BOP	Host IPS	McAfee Network Security Platform	McAfee Vulnerability Manager	McAfee Web Gateway	McAfee Remediation Manager	McAfee Policy Auditor	MNAC
MTIS10-088-A Apple SAF WPC RCE	Previous	Medium	Part	N/A	N/A	Yes	Pend	Part	N/A	Pend	Pend
	Current	Medium	Part	N/A	N/A	Yes	Yes	Part	N/A	Pend	Pend
MTIS10-090-S Adobe 2010-1294	Previous	Low	UA	N/A	N/A	N/A	UA	UA	N/A	Pend	Pend
	Current	Low	UA	N/A	N/A	N/A	N/A	UA	N/A	Pend	Pend
MTIS10-090-T Adobe 2010-1293	Previous	Low	UA	N/A	N/A	Yes	UA	UA	N/A	Pend	Pend
	Current	Low	UA	N/A	N/A	Yes	Yes	UA	N/A	Pend	Pend
MTIS10-090-U Adobe 2009-3467	Previous	Low	UA	N/A	N/A	Yes	UA	UA	N/A	Pend	Pend
	Current	Low	UA	N/A	N/A	Yes	Yes	UA	N/A	Pend	Pend
MTIS10-095-A HP NNM Remote Code Vuln	Previous	Low	UA	UA	UA	UA	UA	UA	UA	UA	UA
	Current	Low	UA	UA	UA	UA	Yes	UA	N/A	UA	UA
MTIS10-095-B MS Win CanDR RC 2028859	Previous	Low	N/A	N/A	N/A	N/A	Pend	N/A	N/A	UA	UA
	Current	Low	N/A	N/A	N/A	N/A	Yes	N/A	N/A	UA	UA
MTIS10-101-B Adobe APSB10 1296	Previous	Medium	UA	UA	UA	UA	UA	UA	N/A	UA	UA
	Current	Medium	UA	UA	UA	UA	UA	UA	N/A	Pend	Pend

Apple Safari 'Window.Parent.Close()' Code Execution Vulnerability [MTIS10-088-A]

Threat Identifier(s)	Apple Safari 'Window.Parent.Close()' RCE
Threat Type	Vulnerability
Risk Assessment	Medium
Main Threat Vectors	Web
User Interaction Required	Yes

Description	A vulnerability in some versions of Apple Safari can lead to remote code execution. The flaw is specific to some uses of the Window.Parent.Close() function. Exploitation can occur via a specially crafted web page and allow an attacker to take remote control of a system.
Importance	Medium. Details of this vulnerability have been publicly disclosed.
McAfee Product Coverage *	
DAT files	Coverage is provided as JS/Exploit-BO.gen in the 5882 DATs, released February 4, for some but not all exploits.
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	The sigset release of May 11 includes the signature "HTTP: Apple Safari window.parent.close Remote Code Execution Vulnerability," which provides coverage.
McAfee Vulnerability Manager	The FSL/MVM package of May 10 includes a vulnerability check to assess if your systems are at risk.
McAfee Web Gateway	Partial coverage is provided in the 7010.7090.2571 Gateway Anti-Malware database update.
McAfee Remediation Manager	Coverage not warranted
McAfee Policy Auditor	Coverage will be provided in the June package release.
MNAC	Coverage will be provided in the June package release.
Additional Information	US-CERT: Apple Safari Vulnerability

Back to top

Adobe ColdFusion Information Disclosure Vulnerability (APSB10-11) [MTIS10-090-S]

Threat Identifier(s)	CVE-2010-1294;APSB10-11
Threat Type	Vulnerability
Risk Assessment	Low
Main Threat Vectors	Web; E-Mail
User Interaction Required	Yes
Description	An information disclosure vulnerability exists in some versions of Adobe ColdFusion. Exploitation requires local access and authentication and may result in the disclosure of sensitive information.
Importance	Low. On May 11, Adobe released an update to address this issue.
McAfee Product Coverage *	
DAT files	Under analysis
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	Coverage not warranted
McAfee Vulnerability Manager	Coverage not warranted
McAfee Web Gateway	Under analysis
McAfee Remediation Manager	Out of scope
McAfee Policy Auditor	Coverage will be provided in the June package release.
MNAC	Coverage will be provided in the June package release.
Additional Information	Adobe: Security update: Hotfixes available for ColdFusion

Back to top

Adobe ColdFusion Admin Page Cross Site Scripting Vulnerability (APSB10-11) [MTIS10-090-T]

Threat Identifier(s)	CVE-2010-1293;APSB10-11
Threat Type	Vulnerability
Risk Assessment	Low
Main Threat Vectors	Web; E-Mail

User Interaction Required	Yes
Description	A cross-site scripting vulnerability exists in some versions of Adobe ColdFusion. The flaw is specific to a vulnerable condition in the ColdFusion Administrator page. Exploitation could lead to cross-site scripting.
Importance	Low. On May 11, Adobe released an update to address this issue.
McAfee Product Coverage *	
DAT files	Under analysis
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	The sigset release of March 14, 2006, includes the signature "HTTP: Cross Site Scripting--Script Attempt Found in HTTP request," which provides coverage.
McAfee Vulnerability Manager	The FSL/MVM package of May 12 includes a vulnerability check to assess if your systems are at risk.
McAfee Web Gateway	Under analysis
McAfee Remediation Manager	Out of scope
McAfee Policy Auditor	Coverage will be provided in the June package release.
MNAC	Coverage will be provided in the June package release.
Additional Information	Adobe: Security update: Hotfixes available for ColdFusion

Back to top

Adobe ColdFusion App Method Cross-Site Scripting Vulnerability (APSB10-11) [MTIS10-090-U]

Threat Identifier(s)	CVE-2009-3467;APSB10-11
Threat Type	Vulnerability
Risk Assessment	Low
Main Threat Vectors	Web; E-Mail
User Interaction Required	Yes
Description	A cross-site scripting vulnerability exists in some versions of Adobe ColdFusion. The flaw is specific to a condition in the ColdFusion method. Targeting applications using this method may result in cross-site scripting.
Importance	Low. On May 11, Adobe released an update to address this issue.
McAfee Product Coverage *	
DAT files	Under analysis
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	The sigset release of March 14, 2006, includes the signature "HTTP: Cross Site Scripting--Script Attempt Found in HTTP request," which provides coverage.
McAfee Vulnerability Manager	The FSL/MVM package of May 12 includes a vulnerability check to assess if your systems are at risk.
McAfee Web Gateway	Under analysis
McAfee Remediation Manager	Out of scope
McAfee Policy Auditor	Coverage will be provided in the June package release.
MNAC	Coverage will be provided in the June package release.
Additional Information	Adobe: Security update: Hotfixes available for ColdFusion

Back to top

HP OpenView Network Node Manager (OV NNM) Arbitrary Remote Code Execution Vulnerability (CVE-2010-1553) [MTIS10-095-A]

Threat Identifier(s)	CVE-2010-1553
Threat Type	Vulnerability
Risk Assessment	Undetermined

Main Threat Vectors	LAN; WAN
User Interaction Required	No
Description	A vulnerability in some versions of HP Network Node Manager can lead to remote code execution. The flaw lies in the getnnmdata.exe CGI. If this CGI is requested with an invalid MaxAge parameter, a sprintf() call is made to log the error. However, no length check is performed on the variable contents before copying into a fixed-length stack buffer. This can be leveraged by remote attackers to execute arbitrary code under the context of the web server process.
Importance	Low. Details of this vulnerability have been publicly disclosed.
McAfee Product Coverage *	
DAT files	Under analysis
VSE BOP	Under analysis
Host IPS	Under analysis
McAfee Network Security Platform	Under analysis
McAfee Vulnerability Manager	The FSL/MVM package of May 19 includes a vulnerability check to assess if your systems are at risk.
McAfee Web Gateway	Under analysis
McAfee Remediation Manager	Out of scope
McAfee Policy Auditor	Under analysis
MNAC	Under analysis
Additional Information	http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02153379

Back to top

Microsoft Windows Canonical Display Driver Code Execution Vulnerability (2028859) [MTIS10-095-B]

Threat Identifier(s)	CVE-2009-3678
Threat Type	Vulnerability
Risk Assessment	Medium
Main Threat Vectors	Web; E-Mail
User Interaction Required	No
Description	A vulnerability in some versions of the Microsoft Canonical Display Driver can lead to remote code execution. The flaw lies in the driver's failure to properly parse information when copied from user mode to kernel mode. Exploitation can occur via a specially crafted image file and allow an attacker to execute arbitrary code.
Importance	Low. Details of this vulnerability have been publicly disclosed.
McAfee Product Coverage *	
DAT files	Coverage not warranted
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	Out of scope
McAfee Vulnerability Manager	The FSL/MVM package of May 19 includes a vulnerability check to assess if your systems are at risk.
McAfee Web Gateway	Coverage not warranted
McAfee Remediation Manager	Coverage not warranted
McAfee Policy Auditor	Under analysis
MNAC	Under analysis
Additional Information	http://vil.nai.com/vil/content/v_vul52433.htm http://www.microsoft.com/technet/security/advisory/2028859.mspx

Back to top

Adobe Photoshop ABR File Processing Buffer Overflow Vulnerability [MTIS10-101-B]

Threat Identifier(s)	CVE-2010-1296
Threat Type	Vulnerability
Risk Assessment	Medium
Main Threat Vectors	Web; E-Mail
User Interaction Required	Yes
Description	A buffer overflow vulnerability in some versions of Adobe Photoshop can lead to remote code execution. The flaw is specific to an input validation error that can arise while processing specific ABR files. Exploitation can occur via a specially crafted ABR file and allow an attacker to execute arbitrary code.
Importance	Medium. Details of this vulnerability have been publicly disclosed.
McAfee Product Coverage *	
DAT files	Under analysis
VSE BOP	Under analysis
Host IPS	Under analysis
McAfee Network Security Platform	Under analysis
McAfee Vulnerability Manager	Under analysis
McAfee Web Gateway	Under analysis
McAfee Remediation Manager	Out of scope
McAfee Policy Auditor	Coverage will be provided in the June package release.
MNAC	Coverage will be provided in the June package release.
Additional Information	Adobe: Security update available for Adobe Photoshop CS4

Back to top

Detailed descriptions of the Security Advisories can be found in the Users Guide:
https://kc.mcafee.com/content/mtis/McAfee_Avert_Labs_Security_Advisory_UsersGuide.pdf

For more information on McAfee Avert Labs Security Advisories, see:
https://kc.mcafee.com/content/mtis/McAfee_Avert_Labs_Security_Advisory_FAQ.pdf

For McAfee Technical Support, click here.

For Multi-National Phone Support, click here.

McAfee values your feedback on this Security Advisory. Please reply to this mail with your comments.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054 888.847.8766 www.mcafee.com