

McAfee Avert® Labs

Security Threat Advisory



December 17, 2008

MTIS08-212

Executive Summary

Since the last McAfee® Avert® Labs Security Advisory (December 17), the following noteworthy events have taken place:

- A patch is now available for the following vulnerability:
 - (MS08-078) Security Update for Internet Explorer (960714)

McAfee product coverage for these events:

McAfee Product Coverage Updates *									
Threat	Advisory	Importance	DAT	BOP	Host IPS	Intru-Shield	Foundstone	MNAC	V-Flash
MTIS08-206-A MS IE XML RCE	Previous	High	Part	Part	Part	Yes	Yes	Yes	Pend
	Current	High	Part	Part	Part	Yes	Yes	Yes	Yes

Microsoft Internet Explorer Nested XML Code Execution Vulnerability [MTIS08-206-A]

Threat Identifier(s)	MS08-078; CVE-2008-4844
Threat Type	Vulnerability
Risk Assessment	High
Main Threat Vectors	E-Mail; Locally logged-on user; Web
User Interaction Required	Yes
Description	A vulnerability in Microsoft Internet Explorer may allow remote code execution. Exploitation would require users to visit a website that has specially crafted, nested XML tags.
Importance	High. On December 17, Microsoft released a patch to address this issue.
McAfee Product Coverage *	
DAT files	Coverage for known exploits is provided as Exploit-XMLhttp.d in the 5459 DATs, released December 9.
VSE BOP	Buffer overflow protection is expected to cover some, but not all, known exploits.
Host IPS	Buffer overflow protection is expected to cover some, but not all, known exploits.
IntruShield	Coverage is provided in the "HTTP: Microsoft Internet Explorer Nested XML Code Execution Vulnerability II" UDS, released on December 16. Previous sigsets provide partial coverage under "HTTP: Possible attempt to create javascript shellcode," released June 28, 2007, and "HTTP: Microsoft Internet Explorer Nested XML Code Execution Vulnerability," released December 9.
Foundstone	The FSL package of December 9 includes a vulnerability check to assess if your systems are at risk.
MNAC	The MNAC release of December 10 includes a vulnerability check to assess if your systems are at risk.

V-Flash	The Remedy V-Flash of December 17 contains remedies for Windows.
Additional Information	McAfee VIL: MS08-078 - Microsoft Internet Pointer Reference Memory Corruption Vulnerability - 960714 http://www.microsoft.com/technet/security/bulletin/ms08-078.msp

[Back to top](#)

Detailed descriptions of the Security Advisories can be found in the Users Guide:
http://knowledge.mcafee.com/solution/mtis/McAfee_Avert_Labs_Security_Advisory_UsersGuide.pdf

For more information on McAfee Avert Labs Security Advisories, see:
http://knowledge.mcafee.com/solution/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.

*The information provided is only for the use and convenience of McAfee's customers in connection with their McAfee products, and applies only to the threats described herein. McAfee product coverage statements are limited to known attack vectors and should not be considered comprehensive. THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS IS" AND IS SUBJECT TO CHANGE WITHOUT NOTICE.

The information contained herein is the property of McAfee, Inc. and may not be reproduced or disseminated without the expressed written consent of McAfee, Inc.

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the United States and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

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

© 2008 McAfee, Inc. All rights reserved.