

## COT Security Alert – Internet Explorer Vulnerability

---

Microsoft has released Security Advisory 979352 for a vulnerability found in Microsoft Internet Explorer which could allow an attacker to take control of an affected system. No Microsoft patches are available for this vulnerability at this time, and Microsoft reports that the vulnerability is being actively exploited on the Internet. This vulnerability is present in Internet Explorer 6, Internet Explorer 7 and Internet Explorer 8 and poses a high risk for all sizes of networks and all home users.

McAfee dat files 5860, 5861 and 5862 address known malware associated with this attack.

If an exploit is successful, an attacker may gain the same user rights as the local user which may allow the attacker to install programs; create new accounts; or view, change or delete data. A denial-of-service may occur if an attempted exploit fails. An exploit can occur by a user accessing a specially crafted website which may appear as an attachment to an email, in an instant message or as an ad on some websites.

Some suggestions and recommendations to minimize the effects of an exploit on the network include:

- Run all software as a non-privileged user (one without administrative privileges).
- Ensure all antivirus and software is current on updates.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Disable Active Scripting in the Internet and Local Intranet security zones.
- Ensure that the Internet Explorer security setting for Microsoft Server 2003 and Microsoft Server 2008 is on High (which is the default setting).
- Ensure that Microsoft Outlook settings allow for HTML sites to open in Restricted Sites setting only (which is the default setting).
- Enable Data Execution Prevention (DEP) for Internet Explorer 6 Service Pack 2 or Internet Explorer 7. (The default setting for this is OFF for IE6 and IE7)

Inform the COT Security Administration Branch if any user is believed to have been affected by an exploit of this vulnerability.

Microsoft and US-CERT have posted information on the vulnerability which can be found on the following links:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/979352.mspx>

<http://blogs.technet.com/msrc/archive/2010/01/14/security-advisory-979352.aspx>

US-CERT:

[http://www.us-cert.gov/current/index.html#microsoft\\_releases\\_security\\_advisory\\_979352](http://www.us-cert.gov/current/index.html#microsoft_releases_security_advisory_979352)

<http://www.kb.cert.org/vuls/id/492515>

McAfee:

<http://www.avertlabs.com/research/blog/>

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

**Security Administration Branch  
Commonwealth Office of Technology  
120 Glenn's Creek Road, Jones Building  
Frankfort, KY 40601**

[COTSecurityServicesISS@ky.gov](mailto:COTSecurityServicesISS@ky.gov)

<http://technology.ky.gov/security/>

