

## Urgent COT Security Alert – Internet Explorer Exploited Vulnerability

---

COT released an alert last week concerning Microsoft Security Advisory 979352 which warns of a vulnerability found in Microsoft Internet Explorer. An exploit of this vulnerability could allow an attacker to take control of an affected system. Microsoft has not released patches for this vulnerability at this time, but intends to release a patch on **January 21st, 2010**. 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.

COT has taken action and blocked several sites associated with exploits of this vulnerability including the following. *(The format has been changed to prevent accidental activation of the link).*

ftpassess[dot]cc  
google[dot]homeunix[dot]com  
tyuqwer[dot]dyndns[dot]org  
blogspot[dot]blogspot[dot]org  
voanews[dot]ath[dot]cx  
360[dot]homeunix[dot]com  
ymail[dot]ath[dot]cx  
yahoo[dot]8866[dot]org  
sl1[dot]homelinux[dot]org  
members[dot]linode[dot]com  
ftp2[dot]homeunix[dot]com  
update[dot]ourhobby[dot]com  
filoups[dot]info

**It is recommended that any agencies or entities that do not utilize the COT content filtering system block these sites at all points necessary to prevent access from the network.**

**While McAfee has issued dat files against known malware associated with this attack, the exploits and sites are dynamic and still pose a threat.**

If an exploit is successful, an attacker may gain the same user rights as the local user, which could include administrator rights. 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:

- Patch systems as soon as the Microsoft out-of-band patch is available after testing according to your procedures.
- 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/>

