

[http://www.pcpro.co.uk/news/news\\_story.php?id=86004](http://www.pcpro.co.uk/news/news_story.php?id=86004)



**COMPUTING IN THE REAL WORLD**





---

SEARCH FOR:

IN: **All IT Sites**

Advanced Search

Guest Level 00

---

**NEWS**

Latest News  
Hot Topics  
News Archive

**PRODUCT REVIEWS**

Latest Reviews  
Reviews Archive  
Labs  
A List

**SHOPPING**

Deal of the Week  
Classifieds

**ANALYSIS**

Columns  
Features  
Real World Computing  
Research Papers

**INTERACTIVE**

IT Forums  
Competitions  
Scrapbook  
Pro Sweep

**DOWNLOADS**

Business  
Graphics  
Desktop  
Music  
Internet  
PDA Zone  
Utilities  
Web Development

**FOCUS ON...**

Broadband  
Digital Cameras  
Security  
Processors  
Operating Systems

**USEFUL INFO**

FAQ

**MAGAZINE**

Subscribe Now  
Change Subscription  
Latest Issue

**FREE NEWSLETTER**

Register for your free weekly newsletter here

Home > News

## News [Security]

Wednesday 12th April 2006

---

### Microsoft fills holes in big April security fix 11:11AM

Microsoft has released five patches covering multiple security vulnerabilities in Internet Explorer in addition to flaws in Windows Explorer, Outlook Express, FrontPage Server Extensions and Data Access Components.

The patches includes a cumulative fix IE which addresses the high profile 'CreateTextRange' flaw. This particular fix will be welcome to many businesses worried about tales of exploits circulating ever since the bug was [publicly disclosed in March](#).

Just days later, [numerous websites](#) were discovered that had been set up to exploit the flaw.

Although security companies offered temporary fixes, Microsoft advised against using them and instead to wait until it had thoroughly tested the patch it was working on. eEye Digital has said that the patch it offered to fix the CreateTextRange flaw is compatible with Microsoft's update and will offer to uninstall once the update is complete.

However, even as Microsoft patches up its products, more holes are being discovered. This time, security company Finjan - in which Microsoft has an investment - reports a bypass and cross zone scripting vulnerability in the Remote Data Service (RDS) object affecting Internet Explorer on Windows, including those updated to Service Pack 2 and also the latest beta version of IE 7.

However, information on the vulnerability, which could allow an attacker remote access to a system and the ability to run code on the target machine, is being disclosed responsibly: ie only Finjan and Microsoft have the full details and are already working on a fix.

Microsoft's five security patches for April comprise:

**Security Bulletin MS06-013** details nine critical vulnerabilities in Internet Explorer 5.01, 5.5 and 6.x. The vulnerabilities could be exploited by malicious people to conduct cross-site scripting attacks, conduct phishing attacks, or compromise a user's system. These are:

An error in the cross-domain restriction when accessing properties of certain dynamically created objects can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site via a JavaScript URI handler applied on a dynamically created "object" tag.

An error within the handling of multiple event handlers (e.g. onLoad) in an HTML element can be exploited to corrupt memory in a way that may allow execution of arbitrary code.

An error within the parsing of specially crafted, non-valid HTML can be exploited to corrupt memory in a way that allows execution of arbitrary code when a malicious HTML document is viewed.

An error within the instantiation of COM objects that are not intended to be instantiated in

**Microsoft Offers**

Register Now & Bid for Microsoft Products on eBay

---

**Latest News**

Toshiba launches first HD DVD laptop

---

CD sales rocket despite digital success

---

Eclipse shadows 8meg Net rollout

---

UK games chart: Lara Croft raids again

---

Microsoft betas Windows Live Academic Search

---

PlusNet rolls out 8meg services from £14.99 a month

---

RealNetworks calls for a Linux DRM

---

Scientists polish diamond transistors

---

W3C moves towards new Cascading Style Sheets standard

---

Microsoft fills holes in big April security fix

[See more News](#)

---

**Hot Topics**

Dual-Core Processors  
Toshiba launches first HD DVD laptop

---


Software Patents  
Patent system in desperate need of overhaul - analyst

---

Wireless  
Korea to create all-standard mobile city

---

Music file-swapping  
UK album charts adopt digital sales


[http://www.pcpro.co.uk/news/news\\_story.php?id=86004](http://www.pcpro.co.uk/news/news_story.php?id=86004)



ADVERTISEMENT

characters in specially crafted URLs can be exploited to corrupt memory in a way that allows execution of arbitrary code. Successful exploitation requires that the system uses double-byte character sets.

An error in the way IOleClientSite information is returned when an embedded object is dynamically created can be exploited to execute arbitrary code in context of another site or security zone.

An unspecified error can be exploited to spoof information displayed in the address bar and other parts of the trust UI.

Some unspecified vulnerabilities exist in the two ActiveX controls included with Danim.dll and Dxtmsft.dll.

[Security Bulletin MS06-014](#) details the critical Microsoft Data Access Components RDS.Dataspace ActiveX Vulnerability.

The vulnerability is caused due to an unspecified error in the behaviour of the RDS.Dataspace ActiveX control as it fails to ensure that it interacts safely with a website and can be exploited by malicious people to compromise a vulnerable system.

[Security Bulletin MS06-016](#) concerns an important vulnerability in Outlook Express versions 5.5 and 6.

The vulnerability is caused due to a boundary error when parsing Windows Address Book (.wab) files. This can be exploited to cause a buffer overflow if a user is tricked into opening a specially crafted .wab file and can be exploited by malicious people to compromise a user's system.

[Security Bulletin MS06-015](#) details a critical vulnerability in Windows Explorer.

The vulnerability is caused due to an error in Windows Explorer when handling of COM objects. This can be exploited to execute arbitrary code by tricking a user into connecting to a malicious file server. Successful exploitation requires that a netbios/CIFS connections can be established.

Finally, [Security Bulletin MS06-017](#) reports a moderate vulnerability in FrontPage Server Extensions. Unspecified input is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

Patches for all the vulnerabilities are available from [www.microsoft.com/security](http://www.microsoft.com/security).

Microsoft has also released an update for its Malicious Software Removal Tool.

Simon Aughton and Matt Whipp

Read comments: 0

Add comments

Email a friend

Add to Scrapbook

#### Related News

- Two new vulnerabilities announced for Windows and IE
- Real patches critical flaws in its media players
- Microsoft issues April security updates
- Media Player exploit found on the Internet

Internet Explorer can be exploited to corrupt memory in a way that allows execution of arbitrary code.

An error within the handling of HTML elements containing a specially crafted tag can be exploited to corrupt memory in a way that allows execution of arbitrary code.

An error within the handling of double-byte

› See more Hot topics

#### Columns



**Computing in the imaginary world:** Dick Pountain takes the notion of theoretical hotels to infinity and beyond - and computers › [See full Opinion](#)

› See more Columns

#### Research Papers

**The Evolution of Support: The Pervasive Service Desk**

**Automate Routine Development Tasks for Improved Application Quality**

**Proven Compatible SAS Solutions - Give You the Flexibility and Scalability to Succeed**

**Who goes there: Securing wireless access**

**I'll be watching you: Wireless IDS/IPS**

› See more Research Papers

[http://www.pcpro.co.uk/news/news\\_story.php?id=86004](http://www.pcpro.co.uk/news/news_story.php?id=86004)

---

Sponsored Links

**Register Now & Bid for Microsoft Products on eBay**

Buy and sell computers and accessories on [eBay.co.uk](http://eBay.co.uk), the UK's online marketplace.

---

[Back to top](#)

---

[Privacy Statement](#) | [Privacy Policy](#) | [Company Website](#) | [Contact Us](#) | [Media Information](#)



© Copyright Dennis Publishing Limited licensed by Felden

Our Other Websites: [Total Gambler](#) | [Inside Edge](#) | [Poker Player](#) | [Bizarre](#) | [Viz](#) | [Auto Express](#) | [Evo](#) | [Test Drive](#) | [Computer Buyer](#) | [Computer Shopper](#) | [Custom PC](#) | [MacUser](#)

---