NEWS BRIEF

Presented by **Crendon Insurance Brokers Ltd**

Internet Explorer's Use-after-free Vulnerability

Just a couple of weeks after news about the Heartbleed bug wreaked havoc in the Internet security world, another serious vulnerability has been discovered, this time affecting Microsoft's Internet Explorer (IE).

This particular flaw is a 'use-after-free' vulnerability, allowing hackers to inject malware into certain websites and then trick users into visiting those websites through spam emails or social engineering. The hackers can then gain total access of a user's system, and from there they can install more malware and view, change or delete data. The more administrative privileges a user has, the worse a possible attack can be.

Hackers often use Adobe Flash Player as a gateway for an attack. Note that the vulnerability is not in Flash itself—the vulnerability relies on an IE flaw that is used to corrupt Flash and bypass Windows security protection.

Are You Affected?

IE versions 6, 7, 8, 9, 10 and 11 are all affected, although attacks are currently targeting versions 9, 10 and 11. However, that does not mean versions 6-8 are safe. 2013 data shows that targeted IE versions account for just over a quarter of the Internet browser market share. Including IE versions 6-8, IE accounts for more than half of the world's browser market share. Currently, all users of IE versions 6-11 are at risk.

How Can You Fix the Problem?

On Thursday, 1 May, Microsoft issued a patch for the vulnerability. The patch is automatically enabled on the computers of individuals who use a Windows operating system and have the automatic update feature turned on. Users who don't have the feature turned on are advised to manually update their computers immediately by checking for Windows updates and installing them.

The patch also includes a fix for Windows XP users, even though Microsoft officially discontinued support for the operating system in early April. This is welcome news because according to a recent AppSense study, 77 per cent of British businesses are still using Windows XP.

What Should Employees, Friends and Family Do?

Alert all friends, family and employees about the vulnerability and recommend that they enable the Microsoft patch immediately, if it hasn't already been done on their computer. Also, remind them of the dangers of clicking on suspicious links or downloading unfamiliar attachments in their email programs.

Crendon Insurance Brokers