



Non-Security Related: Classifying Fixes

infectionvectors.com

March 2006

Overview

Software vendors have always released performance-related patches. These types of updates often solve usability problems, program errors, etc. Depending on one's definition of security, these types of fixes may be considered security-related or non-security-related. This article examines the nature of one such release from Microsoft and the implications of defining the patches within the security dichotomy.

Active

In February of 2006, Microsoft released an advisory for Internet Explorer.¹ The bulletin describing the release is somewhat confusingly titled: "Microsoft Security Advisory (912945): Non-Security Update for Internet Explorer."² There was no new patch associated with the advisory itself; however, two patches that were recently released are discussed. The concern of this article is over the "non-security" update itself, an update to the way IE handles calls to add-on components.

In summary, the patch referenced changes the way ActiveX controls are loaded. Previously, a developer had a number of options as to how to automatically call and employ their control when a browser required them. A few examples of applications that use such IE-entwined controls are Adobe Acrobat Reader, Macromedia's Flash, Microsoft's Media Player, and Apple's Quicktime. In updated versions of IE 6, there is a new requirement for calling such controls, a method that has been described for months on MSDN.

Here is the text from the MSDN notice about the release:

Information for Developers about Internet Explorer
Updated December 2, 2005

After a forthcoming update, Microsoft Internet Explorer users will not be able to directly interact with Microsoft ActiveX controls loaded by the APPLET, EMBED, or OBJECT elements. Users will be able to interact with such controls after activating their user interfaces. A new MSDN topic describes how Internet Explorer will handle ActiveX controls, shows how to load ActiveX controls so their interfaces are activated, and describes the impact of this behavior on accessibility tools and applications hosting the WebBrowser Control.³

Note that there are still mechanisms available to legitimate and malicious coders that wish to make controls active without user intervention. Hopefully, the net result of such changes makes the browser more secure, regardless of how the patch is released. In either case, there is no mention of browser “hardening” in the developer releases, indicating again that this is not considered a security patch, although the impact of the new code would seem to be a defensive action.

ActiveX has long been derided as a security concern (to put it mildly) for many analysts.⁴ The use of the technology has been pointed out as a negative quality when Internet Explorer is compared to other browsers. Security analysts have advised disabling ActiveX in many cases while surfing the Web.⁵ There is a long history of concern over ActiveX’s exploitability. So, there is an obvious tendency to consider any patch to the system in a security context – however that is not what Microsoft appears to intend to present.

To be clear, the Microsoft advisory is intended to alert customers about two distinct patches that were released for IE during the month of February 2006: the fix noted above and MS06-004. The company considered the latter a “security” patch. The “non-security” patch is not a new concept from Microsoft, in September of 2005 there was a “non-security” high priority update for Windows.⁶

Framing

Does the type of release for such a patch affect the priority of the update? It would certainly seem that calling a patch a “security” fix would give it precedence over any “performance” related patches. There a number of reasons for this:

- Time involved in testing patches
- Expense of lab-testing all updates/deployment scenarios
- Risk involved in releasing patch to network machines
- Administrator resistance to change without cause

But the most significant reason may be that the performance patches do not receive a criticality rating. On the scheduled release dates, it is the “Critical” fixes that get the most attention from analysts.

Of course, any type of performance patch could be considered as an important part of proper information assurance practices. The “eye of the beholder” argument could easily be that anything that affects performance affects the availability of the system – one of the pillars of the traditional security model.⁷ Moreover, many fixes are directed in actually correcting errors in the software – which may have direct implications for system integrity. This argument can be applied to virtually any component within an enterprise, from a tiny patch to the hardware selected in a server room to the material used in the walls of that server room.

The area of interest for security researchers is clearly how to define the entire scope of the discipline. There is a longstanding idea that everything is touched by security. If that is true, then security is not so much a discipline in itself as it is a meta-discipline, something that everyone needs to learn about to truly understand how to do their jobs. That bodes both well and poorly for the traditional security manager. Certainly there is no indication that short-term employment will be a problem, but it may mean that in the future the security professional will need to have a specialization in the marketplace to be an effective contributor. Of course, the latter assumes that the world of enterprise IT organizations will correct many of the deficiencies they currently have in security (awareness, matching budgets with risks, etc.). The only people that will be able to affect that change are the security professionals of today. The question before those professionals is how they define their profession, what entails a security concern, and how those concerns are communicated without overburdening management.

Infectionvectors.com provides a number of resources to organizations of all sizes that are looking to expand their security posture. Please visit <http://www.infectionvectors.com> for more information.

References

1. "Information for Developers about Internet Explorer." Microsoft Developers Network. December 2, 2005.
<http://msdn.microsoft.com/ieupdate/>
2. "Microsoft Security Advisory (912945): Non-Security Update for Internet Explorer." February 28, 2006.
<http://www.microsoft.com/technet/security/advisory/912945.msp>
3. "Microsoft Knowledge Base Article 912945: Internet Explorer ActiveX Update." February 28, 2006.
<http://support.microsoft.com/kb/912945>
4. "Renewed browser wars: IE vs. Firefox." ZDNet Robert Vamosi, November 9, 2004.
http://reviews-zdnet.com/4520-3000_16-5561073-1.html
5. "US-CERT: Beware of IE." Internet News. Ryan Naraine, June 29, 2004.
<http://www.internetnews.com/security/article.php/3374931>
6. Non-security patch in September 2005
Brain Krebs "Security Fix – Microsoft Nixes Fix for Black Tuesday." Washington Post. September 9, 2005.
http://blogs.washingtonpost.com/securityfix/2005/09/microsoft_nixes.html & PC-Doctor Guide: <http://www.pcdoctor-guide.com/wordpress/?p=1071> "Patch Tuesday – change of plan." September 10, 2005.
7. The traditional security model has been reviewed in many sources, it consists of a triangle composed of Confidentiality, Integrity, and Availability.