

Lessons learned from Microsoft's MS06-013 patch

Bob Rudis 2006-04-19

On April 11, 2006, as part of Microsoft's regular "Patch Tuesday," Redmond released [MS06-013](#), a cumulative security patch for Internet Explorer. The patch fixes ten vulnerabilities, some with active exploits in the wild. It also contains a functionality update or change in ActiveX that users who patch via Microsoft Update or Windows Update might not have seen.

This article takes a quick look at the functionality changes in MS06-013, and then discusses the new types of deployment decisions that are being made within enterprise environments in light of this critical Microsoft security patch.

Changing how ActiveX controls work

The functionality update in MS06-013 modifies the way ActiveX controls are handled by Internet Explorer. It's a direct response to a \$521M patent dispute with Eolas, a [patent](#) which covers plugins in Web pages that show multimedia content. There is a [thread on Bugtraq](#) that does a great job of explaining the background behind this dispute.

While the majority of users will not read the vulnerability announcements, Microsoft did include a reference to one of their Knowledge Base articles that detailed the potential issues after installing the update. [KB9212812 states](#) that there will be issues with ActiveX plugins – such as QuickTime, Macromedia, and even Java. Furthermore, some components of enterprise-class software are also impacted. Home users having to jump through an extra hoop to play a video is one thing – core business operations being impacted is quite another. There are many cases where enterprise applications may use these technologies in various ways.

Realizing the potential difficulties, Microsoft further released another Knowledge Base article, [KB917425](#). This one is known as the "Internet Explorer ActiveX compatibility patch." The patch reinstates the expected functionality of ActiveX controls, but requires an additional system reboot in order to take effect. Eventually, in order to comply fully with the patent dispute, the new ActiveX functionality will have to be restored by Microsoft. There is no time frame given, but rest assured it will happen at some point.

While home users are left confused about the changes, enterprise administrators are faced with nothing but bad choices:

1. Deploy the patch across all systems without the compatibility patch
2. Deploy the patch across all systems and selectively deploy the compatibility patch
3. Deploy the patch across all systems, including the compatibility patch
4. Selectively deploy the patch
5. Do not deploy the patch

Security is only effective if it is implemented using risk management principles applied in

the context of keeping the business running. In other words, no business = no revenue = no company = no need for security. With that in mind, security administrators at companies across the globe had to recently make one of the above choices. As we prepare for future situations like this, let's do a short analysis of each of these choices:

Deploy the patch across all systems without the compatibility patch

The first option is to do what most security professionals would like to do – patch all vulnerable systems. This is the cleanest approach since it covers the vulnerability and keeps all impacted systems at the same patch-level. It makes managing patch deployments very straightforward and should provide for the least disruption.

However, it may not be realistic to patch all systems in an enterprise without the compatibility patch. It will break certain functionality and could cause a flood of helpdesk calls for any business applications that are affected. The possibility of a disruption in normal business operations is present, however at least all systems will be safely patched.

Deploy the patch across all systems & selectively deploy the compatibility patch

This choice is a bit harder to make. It first requires a decision on whether to identify systems which will be impacted or just exclude all systems potentially impacted – in this case, Windows XP SP2 and Windows 2003 SP1. These are not exactly uncommon operating systems at many organizations. Once that decision is made, the IT department then needs to have the correct infrastructure tools in place to identify these systems and selectively deploy the patch. This means time, money and resources that should be spent supporting real business IT needs will be spent tracking selective patch deployments.

Another side effect of this approach is that a process needs to be put into place to define these deviations in the event that issues arise as a result of the second patch, expending yet more time, money and resources.

Finally, in the case of this particular second patch, there will need to be two reboots per system deployment causing more than just the usual user frustration.

Deploy the patch across all systems, including the compatibility patch

This option has all of the problems of the previous one, but also increases the likelihood of encountering issues associated with the compatibility patch. While the additional patch was supposed to restore functionality, there is always the potential of modified code to cause problems as well as fix issues. IT/Security departments should ideally test both patches prior to deployment.

Selectively deploy the patch / Do not deploy the patch

While mixing and matching compatibility patch deployments can be challenging, there is a

real security risk involved with only deploying the main patch to a subset of systems - or even not deploying it at all, especially when it is mitigating known, active exploits on the Internet.

IT/Security departments faced with this alternative are not left completely vulnerable, however. There are a number of desktop and server-based firewall, anti-virus and intrusion prevention components that can defend against known exploits and malicious behaviors. However, these programs are meant to be deployed in a layered security solution, with patching of desktops and mobile systems being the foundation of any good security strategy. Relying solely on the ability of security vendors to stay ahead of the attackers is an unenviable position to be in.

The norm instead of the exception

While IT/Security departments have not faced this situation too often, there is real evidence to suspect that this type of debate will become the norm as opposed to the exception, as software patents generate more litigation and require more remediation.

In the case of the ActiveX patch, Microsoft took advantage of the need for users to fix vulnerabilities in order to satisfy a legal issue with the least amount of cost and administrative overhead as possible, while also getting as widespread a deployment as possible.

It is important for IT/Security departments to be ready for this emerging trend by ensuring some fundamental things are in place:

- A comprehensive asset management system to ensure complete knowledge of what's on the network (and ideally, when new devices are added to the network).
- Robust, platform independent patch management tools to make it easier to customize complex deployments
- Solid risk management processes and procedures to allow for fast response to vulnerability announcements and threats
- A layered security strategy on systems and networks to help mitigate risk while tough decisions need to be made

Conclusion

Most organizations are just getting comfortable with regular vulnerability patch management and now have to adjust their thinking yet again. With the right tools and processes in place, however, the decisions may not have to be so quick or as painful as they no doubt were this time.

In this brief article we've looked at some lessons learned from Microsoft's latest MS06-013 security patch. The patching, monitoring, and deployment of Windows security releases in an enterprise environment is already a significant cost, and the new choices IT/Security departments are faced with will only take these costs higher.

[Privacy Statement](#)

Copyright 2006, SecurityFocus