

RE: MS Software Update Service

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-02/0108.html>

From: m0use (m0use@helixsecurity.net)

Date: 02/21/03

From: "m0use" <m0use@helixsecurity.net>

To: "'Starks, Brad'" <BStarks@co.marin.ca.us>, <focus-ms@securityfocus.com>

Date: Thu, 20 Feb 2003 23:23:39 -0600

>*Is it comparable to other solutions like Update Expert, Hfnetchk Pro, Net Octopus, etc.?*

First the disclaimer, I work for a major vulnerability remediation software company to remain nameless. I tried out SUS and it seemed ok, This was just a quick test but I see a few things missing and from other posts in the thread others agree. We need to patch systems, not just operating systems. What about office? And SQL? Can you say SQL Snake? And dare I bring up Linux? Or Solaris? I recommend that people look for a solution not limited by the whims of M\$. Citadel has Hercules, Shavlik has Hfnetchk Pro, St. Bernard has Update Expert. These packages overcome the limitations... I'll summarize the thread as I've read it below.... And in short the Con's far outweigh the Pro's the way I see it.

Pro's

- you get the advantages of Automatic Update (patches pushed to client systems without intervention) with the added bonus that you get to test and approve the patches before releasing them to your clients. (also available in some commercial products)
- If you integrate SUS with Active Directory, it gives you even greater control over who gets the patches and when.
- it can be easily controlled using GPOs and relies on administrative approval of updates
- simple installation, downloaded, installed, synchronized the updates
- free

Con's

- only works with Win2K and XP clients (i.e., that can support the Automatic Update client)
- only distributes patches for Windows OS, IE, IIS and (I believe) Windows Media Player - in other words, the OS and any apps that come "bundled" with the OS. Doesn't patch SQL Server, Exchange, Office, etc.
- cannot install Service Packs (though note that Service Packs can be distributed through Active Directory software installation, so this may not matter to you)

SecurityFocus Microsoft: RE: MS Software Update Service

- it is a pull system... the client system has to pull the patches from the server, rather than getting them pushed out.
- It would be nice if the administration interface would tell me at least a summary of which machines have grabbed what and when.
- lacking in several features that most enterprises would require for a full rollout of this solution. It lacks grouping functions, has no reporting functions, no varying levels of administration, and only provides for updates to Microsoft products.
- The logging also is very basic and requires you to sift through IIS logs looking for HTTP gets from the target host. You can't tell from the server whether a patch has been correctly installed or not and it does not offer a centralized way to back out of a patch application. All in all it didn't come close to meeting our needs.
- is that it doesn't support office or server application updates
- it still leaves admins in the dark on what updates have been applied without extensive scripts to dig out the information.
- For our distributed environment the current version of SMS is not manageable due to its need for domain admin level access.
- M\$ changes their update strategy weekly, Most Vuln Remediation vendors are in this for the long haul. Other than software updates the products should be around a while.
- Only looks at things from M\$'s point of view. Use a good vuln scanner on a freshly "updated" box and see what update missed.

And my vote is for Citadel's Hercules. Multiple platforms (Windows, Linux, Solaris) Works from the results of most major vuln scanners. Independent view of vulnerabilities, doesn't rely on anyone owning up to mistakes. From a vendor that does this for a living. No conflicts of interest and product focused support.