

30 July 2008

By: Marius Oiaga, Technology News Editor

Security
Microsoft

[Microsoft Points the Finger at the Apple OS X Insecure Update Mechanism](#)

And not only

[Robert Hensing](#), Microsoft Security Software Engineer, was quick to point the finger at what he referred to as insecure third party software updaters, offering a "well deserved" fail open goat award to a variety of product makers including Sun and Apple. [Michael Howard](#), a Senior Security Program Manager in the Security Engineering group at Microsoft, pointed out that Hensing was right in indicating the superiority of Microsoft's own updating infrastructure and solutions over those of its rivals when it comes to a malware distribution toolkit available in the wild targeting insecure online updating processes. The ISR-evilgrade v1.0.0 is a toolkit designed to facilitate man-in-the-middle exploits of popular software solutions including the Java plugin, Winzip, Winamp, MacOS, OpenOffices, iTunes, LinkedIn Toolbar, DAP [Download Accelerator], notepad++ and speedbit. And although Windows users are indeed at risk, the attacks will not target Microsoft's operating system or update mechanism directly, they will only do so through faulty third party solutions. "You'll notice Microsoft's auto-updaters (Windows Update / Microsoft Update / Automatic Updates) are not on the list. Why? Because we're paranoid, and we anticipated this type of threat years ago and mitigated it by signing all of our binaries and only allowing our updater to install binaries signed by us. I guess other vendors didn't get the memo," Hensing added. Evilgrade uses the DSN exploit made available by security researcher [H.D. Moore](#), but will only work in tandem with insecure update mechanisms. In this context, used in conjunction with WU, AU or MU, Evilgrade will not permit an attacker to gain control over a target Windows operating system. Bringing software like iTunes, OpenOffice or Winamp into the equation completely changes the problem and exposes users to the exploit. Since the start of July, Microsoft has released a [security bulletin](#) designed to address the DNS Spoofing vulnerability affecting a wide range of Windows platforms including Windows XP SP3. "ISR-evilgrade is a modular framework that allows us to take advantage of poor upgrade implementations by injecting fake updates. It works with modules, each module implements the structure needed to emulate a false update of specific applications/systems. Evilgrade needs the manipulation of the victim DNS traffic," stated the creator of the toolkit, [Francisco Amato](#). "The framework is multiplatform, it only depends of having the right payload for the target platform to be exploited." A video demonstration is available [here](#).