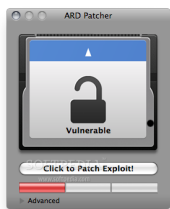


7 July 2008

By: Filip Truta, Apple News Editor

## [ARD Patcher Fixes Apple Remote Desktop Exploit](#)

### *No need for paid antivirus solutions*



Step 1 - the software acknowledges the threat

Over the past few weeks reports talking about this vulnerability connected to Apple's Remote Desktop Agent in Mac OS X have been literally pouring in. Multiple security firms say [the vulnerability](#) allows shell scripts to be run as root - for which they are offering solutions, and costly ones at that. However, developers Youssef Francis and Pepijn Oomen have released [a free patch](#) to resolve the issue and shut everyone up. The vulnerability allows malicious programs to execute code as root when run locally, or via a remote connection, on computers running Mac OS X 10.4 and 10.5. Apple has strangely let this vulnerability "slip," while some reports claim the Mac maker is busy working on a patch. Needless to point out, the fact that two devs have managed to release a patch on such a short notice says a lot about Apple's attitude towards security threats. The patch is as simple to install and run, as it is simple in what it does: *it restricts ARDAgent to the basic applescript dictionaries, preventing use of the "do shell script" command.* The tool is open source under GPLv2, while the source code is provided with [the app](#). "Due to an exploit in Apple's Remote Desktop Agent, a new 'trojan horse' has surfaced for Mac OS X; and with it, appeals from Anti-Virus software companies claiming you need to buy a product to protect yourself," the aforementioned developers note. "The truth: this trojan horse, so far, has not been documented in the wild, and in fact, we find it highly suspicious that multiple Anti-Virus companies have been able to get a hold of it." Youssef Francis and Pepijn Oomen's ARD Patcher is small and easy to install, and guarantees to patch the exploit, free-of-charge. According to the two developers, it's really just "a simple patch that Apple will surly [sic] fix in an upcoming update." Not making any profits with these claims, the developers confidently state that "getting an antivirus program is just overkill in this situation, despite what all the companies that make them will tell you." The ARD Patcher is currently at version 1.1.1. Those who haven't already downloaded and run it should note that the latest release contains an advanced option to disable ARD altogether. Under "Advanced," there is a "remote SetUID Bit option for disabling ARD. If you tick the checkbox the ARD Patcher will remove the setuid bit from ARDAgent, effectively disabling Apple Remote Desktop admin. According to the developers, "this option is a highly precautionary, extra security measure for those who would rather disable ARD admin, than worry about security. It is neither necessary nor recommended unless you know what you are doing." However, you needn't tick the box if you're not that paranoid, as the patch alone restricts the applescript dictionaries for ARDAgent to the default dictionaries. This doesn't include the "do shell script" command, so just installing and running the patch should keep you on the safe side. The free ARD Patcher is available [HERE](#).