INTEGO SECURITY ALERT - June 19, 2008
Apple Remote Desktop Vulnerability
Allows Malicious Programs to Execute Code as Root

Exploit: ARDAgent root privilege escalation

Discovered: June 19, 2008

Risk: Critical

Description: A vulnerability has been discovered that 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. This vulnerability takes advantage of the fact that ARDAgent, a part of the Remote Management component of Mac OS X 10.4 and 10.5, has a *setuid* bit set. Any user running such an executable gains the privileges of the user who owns that executable. In this case, ARDAgent is owned by root, so running code via the ARDAgent executable runs this code as root, without requiring a password. The exploit in question depends on ARDAgent's ability to run AppleScripts, which may, in turn, include shell script commands.

When an application enables a root privilege escalation of this type, any malicious code that is run may have devastating effects. These may range from deleting all the files on the Mac (regardless of who owns them) to more pernicious attacks such as changing system settings, and even setting up periodic tasks to perform them repeatedly. Any application could use this vulnerability to obtain root privileges without users ever needing to enter passwords. Users could run malicious programs that they download from the Internet or receive from friends or colleagues, and, if the program exploits this vulnerability, simply launching it once would be sufficient for damage to be done.

This exploit can be triggered by any type of user account: standard user, administrator, or even a guest account. Therefore, a guest logged in using Mac OS X 10.5's Guest Account feature has the ability to download an application and unwittingly run malicious code with no security warning.

Means of protection: The best way to protect against this exploit is to run Intego VirusBarrier X5 with its virus definitions dated June 19, 2008. VirusBarrier X5 will perform an action that will deactivate ARDAgent's ability to run AppleScripts. Intego recommends that users never download and install software from untrusted sources or questionable web sites.

About Intego

Intego develops and sells Internet security and privacy software exclusively for Macs and iOS devices.

Intego provides the widest range of software to protect users and their Macs and iOS devices from the dangers of the Internet. Intego's multilingual software and support regularly receives awards from Mac magazines, and protects more than one million users in over 100 countries. Intego has headquarters in the USA, France and Japan. For further information, visit www.intego.com.