

Re: Another Mac OS X ScreenSaver Security Issue (after Security Update 2003-07-14)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0423.html>

From: MightyE (trash_at_mightye.org)

Date: 07/31/03

Date: Thu, 31 Jul 2003 16:17:27 -0400

To: David Riley <oscar@the-rileys.net>, bugtraq@securityfocus.com

>a) *If the screensaver engine is compromised (as it was earlier this month, though likely not in a command-execution sort of way), you don't want to be able to give the user root privileges. Presumably, xscreensaver has safeguards against that (or they assume it'll never be exploited). It would be pretty sad to have a root security hole through the screensaver.*

>

>

Yes, this would certainly be pretty sad, but as I see it, the screensaver is one of the most important local (non remote) security devices, it protects against casual cracking attempts of using a restricted application that was left running when someone was called away from their desk. Although a root exploit on the screensaver would be worse than merely crashing the screensaver, neither are tolerable if you ask me, so may as well stress test the screensaver engine till you can rely on it, then trust it with root access.

>b) *Sometimes the screensaver does crash. Keep in mind that since the screensaver modules are executable code (as xscreensaver modules probably are as well, though I've never made one), that's the responsibility of the individual screensaver developer to fix. It's nice to be able to kill it when it does crash so that you can use the computer again.*

>

A developer could add a `--PERMIT_KILL` option while testing their screensaver which would tell Escape Pod that it's ok to kill this process when the request came in. Also if they had a remote terminal up, and root access, they could always kill it that way. As I see it, a user really needs to be able to depend on their screensaver to protect their workstation while they're not at it. A person doesn't necessarily have the option of logging out of their workstation completely when they go away from their desk, nor the time to take other security steps.

It's true that someone having physical access to your machine (and a desire to use such access for evil) gives them a level of control that can't be truly protected against with a screensaver of any calibre, but it does protect the payroll manager from having one of his lackeys give

himself a pay raise while he's at a meeting.

-e