Apple releases update to fix critical macOS High Sierra security issue

Apple has just rolled out a security update for macOS High Sierra that fixes the major flaw that was publicly disclosed yesterday. A for the patch, Security Update 2017–001, confirms that it addresses the vulnerability that allowed admin access to a Mac computer without providing any password.

Apple is urging customers to “install this update as soon as possible” right in the update description, and you should probably heed that advice if you’re running the company’s latest desktop software. Seriously. It’s even in bolded text. Apple is doing its part to make sure the crucial security patch spreads fast: beginning later today, the update will automatically be installed on all systems running High Sierra. That should make life easier for IT administrators.

But Apple is clearly disappointed with itself over this whole thing. It’s a humbling embarrassment for a company that so often highlights its focus on user security and privacy. “Security is a top priority for every Apple product, and regrettably we stumbled with this release of macOS,” Apple said in an unusually forward statement. “We greatly regret this error and we apologize to all Mac users, both for releasing with this vulnerability and for the concern it has caused. Our customers deserve better. We are auditing our development processes to help prevent this from happening again.”




To safeguard your Mac, just open the Mac App Store and you

should see the update available to download. The installation process doesn’t require a restart – or at least it didn’t when I updated moments ago.

The exploit was shared in full detail on Twitter yesterday, prompting Apple to quickly publish step-by-step instructions for protecting against the “root” password loophole. This patch to fully resolve the issue comes less than 24 hours later. And it seems to have been a *very* quick effort; Apple says its security engineers went work when they became aware of the flaw “Tuesday afternoon,” which confirms that the company got no warning before it was publicly revealed.