Apple OSX High Sierra 10.13 authentication bug

Overview

A security flaw has been detected in the Apple OSX operating systems High Sierra 10.13. This flaw allows an attacker with existing access to a Mac to enable the root account with any password, blank has been a popular choice. Once root is enabled, the attacker has complete control and can build on her access, including network access via screen sharing (VNC). More details on how to trigger the bug are in the links section. This bug requires the root account to be disabled, which is the default OSX setting.

Update: A patch was released to fix this issue on Nov 29, 2017.

What should I do?

- Run software update and insure all patches are applied. Here are instruction to run update: https://support.apple.com/en-us/HT201541
- Install the Lab provided BigFix client so that IT can assist you in keep your computer patched and secure. BigFix can be found at https://software.lbl.gov

Resources

Systems at Risk

- Currently, this vulnerability only exists in High Sierra 10.13
- Systems that allow local physical access, such as shared usage computers, computers in lab environments, or laptops that travel
- Systems with Screen Sharing (VNC) enabled

Systems Not at Risk

- Mac operating systems that are prior to 10.13
- Systems using SSH (Secure Shell) since SSH does not allow root access with a password by default.

Links

- Original twitter post: https://twitter.com/lemiorhan/status/935581020774117381
- Detailed technical writeup: https://objective-see.com/blog/blog_0x24.html

Questions

If you have any further questions, please write us at security@lbl.gov