CERT-EU Security Advisory 2017-026

Unauthenticated Root Access in macOS High Sierra

November 30, 2017 — v1.1

History:

- *29/11/2017 — v1.0: Initial publication*
- *30/11/2017 — v1.1: Update resolving the issue is available*

Summary

On November 28th, a security researcher Lemi Orhan Ergin has notified Apple about a serious security issue in macOS Hight Sierra [1]. It appears that anyone can login as *root* by providing an empty password. The bypass works by putting the word *root* in the user name field of a login window, moving the cursor into the password field, and then hitting *Enter* with the password field empty. With that – after a few tries in some cases – the latest version of Apple's operating system logs the user in with root privileges [2].

Interestingly enough, the functionality was already identified and presented as a solution to logging-in problems in a post of user *chethan177* on Apple developer forums already on November 13th [3]. At the time, it appears that nobody felt the need to raise an alert about it.

On November 29th, Apple has released a Security Update 2017-001, which corrects the issue.

Technical Details

When full-disk encryption is turned off, an untrusted user can turn on a Mac that is fully powered down and log in as root. Even on Macs that have filevault turned on, the bypass can also be used to make unauthorized changes to the System Preferences (including disabling filevault), or the bypass can be used to log in as root after logging out of an existing account but not turning off the machine [2].

Of more concern is that malicious hackers can exploit this vulnerability to give their malware unfettered control over the computer and OS. In cases such as these, attackers use one exploit to run their malicious code and a second exploit to escalate the privileges of that code so it can perform actions that the OS normally would not allow [2].

It appears that the vulnerability is located in `com.apple.loginwindow`, a macOS component that is one of at least two ways users can log into accounts [2].

Products Affected

Apparently this bug is present in the current version of macOS High Sierra, 10.13.1, and the macOS 10.13.2 beta that is in testing at the moment [4].

Recommendations

Apple has released an update (Security Update 2017-001) to correct the issue, and it is available through the App Store *Update* tab. The update may be installed manually, and later will also be pushed automatically to the impacted systems. A short description, along with a method to check if the update was applied on a given system is available in [5].

References

[1] https://twitter.com/lemiorhan/status/935578694541770752

[2] https://arstechnica.com/information-technology/2017/11/macos-bug-lets-you-log-in-as-admin-with-no-password-required/

[3] https://forums.developer.apple.com/thread/79235#277225

[4] https://forums.macrumors.com/threads/major-macos-high-sierra-bug-allows-full-admin-access-without-password-how-to-fix-updated.2091696/

[5] https://support.apple.com/en-us/HT208315