

Components:

apple iphone os *
apple ipados *
apple macos *

Description:

A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 16.6.1 and iPadOS 16.6.1, macOS Monterey 12.6.9, macOS Ventura 13.5.2, iOS 15.7.9 and iPadOS 15.7.9, macOS Big Sur 11.7.10. Processing a maliciously crafted image may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Main problems:

120 "Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')"