



Millions of iPhone Users Warned by Federal Agency to Change Settings Immediately

Description

USA: US Cybersecurity and Infrastructure Security Agency says users, admins should update software as soon as possible

Apple Inc. and a top U.S. cybersecurity agency are urging [iPhone](#), iPad, and Macbook users and administrators to update their iOS software following the recent discovery of security vulnerabilities.

“Apple has released security updates to address vulnerabilities in macOS Monterey, iOS and iPadOS, and Safari. An attacker could exploit one of these vulnerabilities to take control of an affected device,” the Cybersecurity and Infrastructure Security Agency (CISA) said in a [statement](#) on Aug. 18.

Users and administrators are urged to review Apple’s security updates [page](#) and apply the updates—MacOS Monterey 12.5.1, iOS 15.6.1, iPadOS 15.6.1, or Safari 15.6.1—as soon as possible.

Apple released [two security reports](#) about the issue on Wednesday, although they didn’t receive wide attention outside of tech publications.

The vulnerabilities could allow hackers to gain “full admin access” to the device.

That would allow intruders to impersonate the device’s owner and subsequently run any software in their name, said Rachel Tobac, CEO of SocialProof Security, in an interview with The Associated Press.

Security experts have advised users to update affected devices—the iPhone6S and later models; several models of the iPad, including the 5th generation and later, all iPad Pro models and the iPad Air 2; and Mac computers running MacOS Monterey. The flaw also affects some iPod models.

Commercial spyware companies such as Israel's NSO Group are known for identifying and taking advantage of such flaws, exploiting them in malware that surreptitiously infects targets' smartphones, siphons their contents, and surveils the targets in real-time.

NSO Group has been blacklisted by the U.S. Commerce Department. Its spyware is known to have been used in Europe, the Middle East, Africa, and Latin America against journalists, dissidents, and human rights activists.

"The flaws were found in the kernel, a program at the core of the OS (CVE-2022-32894) and WebKit, the engine that powers the Safari web browser (CVE-2022-32893). Both flaws allow hackers to remotely execute malicious code on your iPhone, iPad, or Mac and potentially take over your device," according to Forbes tech security writer Gordon Kelly.

How to Update

To update the software on an iPhone, iPad, or iPod touch, go to the Settings section. From there, tap General before tapping Software Update.

Review the update before tapping "download and install" to update the device.

On a Mac computer, go to System Preferences, then click on Software Update before clicking either Update Now or Upgrade Now. Users can also go to the App Store and click on the Updates tab.

featured photo: An Israeli woman uses her iPhone in front of the building housing the Israeli NSO group, in Herzliya, near Tel Aviv, Israel, on Aug. 28, 2016. (Jack Guez/AFP via Getty Images)

by Jack Phillips

Category

1. Crime-Justice-Terrorism-Corruption
2. Freedom-Free speech-Resistance & H-rights
3. Main
4. Science-Tech-AI-Medical & Gen. Research

Date Created

08/24/2022