



## Apple releases new security updates for their products



Apple released multiple security patches for macOS Big Sur, iTunes for Windows and Safari.

The security patches for [Safari cover 2 vulnerabilities](#) (CVE-2020-9945, CVE-2020-27918). The first is an input validation issue, which could be exploited when entering a malicious website who would spoof the URL indicated at the address bar. The second vulnerability could be exploited if Safari processed custom, malicious content which eventually allowed for code execution from within the displayed web content.

Several more vulnerabilities were found and patched in [iTunes for Windows 10](#). These could allow malicious actors to read files from the host (CVE-2020-10002) or execute code due to out-of-bounds writes and improper input validation and processing of images (CVE-2020-27912). As detailed at the security update, the vulnerability seen in the WebKit of Safari can also be exploited also in iTunes, as the WebKit web browser engine is used by apple in all their products (CVE-2020-27918)

Finally, Apples macOS Big Sur had a major update, including security patches. This update is available for both of Apples' previous [X64 devices](#) and the new [RISC-V \(M1\) based devices](#).