SEQURETEK

APPLE - 3 ACTIVELY EXPLOITED ZERO DAYS

OVERVIEW

Apple has patched the three zero-day vulnerabilities with latest release of iOS 14.2.

The three zero-day vulnerabilities were actively exploited in the wild and affecting iPhone, iPad, and iPod devices.

The flaws reside in the FontParser component and the kernel, allowing adversaries to remotely execute arbitrary code and run malicious programs with kernel-level privileges.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
11th Nov 2020	v 1.0	Sameer Prabhu	Mr. Pritish Bharambe

OVERVIEW

- Apple on 5th Nov. 2020, released multiple security updates to patch three zero-day vulnerabilities that were revealed as being actively exploited in the wild, with latest release of iOS 14.2.
- The updated rolled out as part of its iOS, iPadOS, macOS, and watchOS updates fixes flaws in the FontParser component and the kernel which could allow adversaries to remotely execute arbitrary code and run malicious programs with kernel-level privileges.
- The zero-days were discovered and reported to Apple by Google's Project Zero security team.
- The list of impacted devices includes iPhone 5s and later, iPod touch 6th and 7th generation, iPad Air, iPad mini 2 and later, and Apple Watch Series 1 and later.

TECHNICAL DETAILS

- One of the vulnerabilities is a remote code execution (RCE) bug tracked as **CVE-2020-27930** and triggered by a memory corruption issue when processing a maliciously crafted font by the FontParser library.
- The second actively exploited bug is a kernel privilege escalation flaw **CVE-2020-27932** caused by a type confusion issue that makes it possible for malicious applications to execute arbitrary code with kernel privileges.
- The third iOS zero-day is a kernel memory leak tracked as **CVE-2020-27950** and caused by a memory initialization issue that allows malicious applications to gain access to kernel memory.
- All three bugs are believed to have been used together, part of an exploit chain, allowing attackers to compromise Apple devices remotely.
- The zero-days were addressed by Apple earlier today, with the release of iOS 14.2, the mobile OS's latest stable version.
- The same security bugs have also been fixed in iPadOS 14.2 and watchOS 5.3.8, 6.2.9, and 7.1, and have also been backported for older generation iPhones via iOS 12.4.9.

AFFECTED DEVICES

The list of affected devices includes

- iPhone 6s and later
- iPod touch 7th generation
- iPad Air 2 and later running iPadOS versions prior to iOS 14.2
- iPad mini 4 and later
- Macs running macOS Catalina versions prior to macOS Catalina 10.15.7
- Apple Watches running watchOS versions prior to watchOS 7.1, watchOS 6.2.9, watchOS 5.3.9
- Apple TVs running tvOS versions prior to tvOS 14.2

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- It is recommended to patch the vulnerabilities by updating to versions iOS 12.4.9 and 14.2, iPadOS 14.2, watchOS 5.3.9, 6.2.9, and 7.1, and by applying a supplemental update for macOS Catalina 10.15.7.