KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Apple patches two highly exploited zero-days

Tracker ID: TN0826 **Date:** 18/Aug/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

The Apple security update patched two zero-day vulnerabilities that threat actors utilized to exploit iPhones, iPads, and Macs. This patch addresses kernel and Webkit vulnerabilities that could lead to arbitrary code execution. CVE-2022-32893 and CVE-2022-32894 appear to pose a high risk as they are actively exploited.

The releases address the identical issues where CVE-2022-32894 is a kernel flaw that could allow applications to "run arbitrary code with kernel privileges" and CVE-2022-32893, a vulnerability that affects WebKit and allows arbitrary code execution via "maliciously constructed online content." The WebKit is used by the Safari browser and Mail, which use Apple's WebViews for content rendering and display.

Other details about these attacks, as well as the names of the threat actors who carried them out, were not revealed, but they appear to have been used as part of highly targeted attacks. Both the vulnerabilities have been addressed in the most recent versions of iOS 15.6.1, iPadOS 15.6.1, and macOS Monterey 12.5.1.

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-32893	NA	NA
CVE-2022-32894	NA	NA

Affected Products and Versions

- Versions prior to iOS 15.6.1
- Versions prior to iPadOS 15.6.1
- Versions prior to macOS Monterey 12.5.1

Recommendations

- Immediately identify the vulnerable instances and apply the vendor-provided fixes as soon as possible.
- Collect and review relevant logs, data, and artifacts to ensure the threat is eradicated from the network and thwart residual issues that could enable follow-on exploitation.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Apple patches two highly exploited zero-days

Tracker ID: TN0826 **Date:** 18/Aug/2022 **Category:** Vulnerability **Industry:** All **Region**: All

References

- Apple, About the security content of iOS 15.6.1 and iPadOS 15.6.1, 17th August 2022, External Link (support.apple.com).
- Apple, About the security content of macOS Monterey 12.5.1, 17th August 2022, External Link (support.apple.com).
- Johannes Ullrich, Apple Patches Two Exploited Vulnerabilities, SANS, 17th August 2022, External Link (isc.sans.edu).
- Ravie Lakshmanan, Apple Releases Security Updates to Patch Two New Zero-Day Vulnerabilities, The Hacker News, 17th August 2022, External Link (thehackernews.com)
- HKCERT, Apple Products Multiple Vulnerabilities, 18th August 2022, External Link (www.hkcert.org).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471