

Menlo Labs Threat Bulletin

Bulletin: 2022—013

Date: 24/08/2022

Name: Apple 0 Days

Classification: Browser Zero Day - CVE-2022-32893

Summary

Apple has issued a security update with the release [iOS 15.6.1](#), [iPadOS 15.6.1](#) and [macOS Monterey 12.5.1](#) to address a high severity WebKit browser vulnerability CVE-2022-32893.

The vulnerability is confirmed to be exploited in the wild and at the time of this writing, Apple has not yet published details or IOCs for the in the wild exploitation and attacks leveraging the vulnerability.

Infection Vector

The browser zero day is primarily affecting Apple's default browser engine - Safari. The vulnerability is an out-of-bounds write issue in WebKit used by Safari browsers. A successful exploitation of the vulnerability could allow an attacker to perform arbitrary code execution on affected products

Below is a table, listing details of the HIGH severity vulnerability, with associated CVE patched by Apple.

CVE	Severity	Description	In the wild exploitation
CVE-2022-32893	High	Out-of-bounds write issue in WebKit	Yes. Confirmed by Apple.

Menlo Recommendations

Menlo recommends all Apple users to upgrade to iOS 15.6.1, iPadOS 15.6. and macOS 12.5.1 that addresses the vulnerability.

Menlo Protection

Customers using the Menlo Cloud Security Platform are protected against such vulnerabilities by design! With Menlo, when a user visits a website via the isolation platform (including IOS and Android mobile devices), all active content is executed in the Menlo cloud-based isolation platform - Not on the user's device. Menlo protects all devices—including mobile. However, we don't have enough details to state this with certainty.

Menlo labs is actively monitoring for any IOCs and will send updates, once additional details about the threat are identified.