1 650.614.1705
support@menlosecurity.com
www.menlosecurity.com

Menlo labs.

Menlo Labs Threat Bulletin

Bulletin: 2023—01

Date: 17/02/2023

Name: Apple 0 Days

Classification: Browser Zero Day - CVE-2023-23529

Summary

Apple has issued a security update for Safari running macOS Big Sur and macOS Monterey to address a high severity WebKit browser vulnerability CVE-2023-23529.

Apple has not yet published details or IOCs or given any information about 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 a type confusion issue that could allow an attacker to process malicious crafted web content that may lead to 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-2023-23529	High	Webkit type confusion issue	Yes. Confirmed by Apple

Menlo Recommendations

Menlo recommends all Apple users to update to Safari 16.3 that addresses the vulnerability with the build number 167614.4.6.11.6 on macOS Big Sur and 177614.4.6.11.6 on macOS Monterey.

Menlo Protection

Customers using the Menlo Cloud Security Platform are usually 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.

Based on the information available, the Menlo isolation platform would disrupt the exploit chain needed to take advantage of it. Menlo labs is actively monitoring for any further intel and will send updates, once additional details are identified.