

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Apple Addresses Zero-Day Vulnerabilities in macOS and Safari**

Date of Publication

April 11, 2023

Admiralty Code

A1

TA Number

TA2023177







# Summary

**First Seen:** April 7, 2023

**Affected Product:** Apple macOS, Safari

**Impact:** Vulnerabilities in an app processing web content can potentially result in arbitrary code execution with kernel privileges

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-28205	Apple WebKit Use-After-Free Vulnerability	Apple macOS, Safari in macOS Big Sur and macOS Monterey			
CVE-2023-28206	Apple macOS IOSurfaceAccelerator Out-of-Bounds Write Vulnerability	Apple macOS			

# Vulnerability Details

Apple addressed vulnerabilities in macOS Ventura and Safari for macOS Big Sur/Monterey, which could potentially enable attackers to execute arbitrary code with kernel privileges or through processing maliciously crafted web content. These vulnerabilities are being actively exploited. One of the vulnerabilities, identified as CVE-2023-28205, is a use-after-free vulnerability found in WebKit and could enable arbitrary code execution through processing malicious web content. The other vulnerability, CVE-2023-28206, is an out-of-bounds write vulnerability discovered in IOSurfaceAccelerator that could allow attackers to execute arbitrary code with kernel privileges.

# Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-28205	Apple Safari in macOS Big Sur and macOS Monterey: 16.0 - 16.4 macOS Ventura: 13.0 22A380 - 13.3 22E252	cpe:2.3:a:apple:apple_safari:*.:*:*:*:*:* cpe:2.3:o:apple:macos:*.:*:*:*:*:*	CWE-416
CVE-2023-28206	macOS Ventura: 13.0 22A380 - 13.3 22E252	cpe:2.3:o:apple:macos:*.:*:*:*:*:*	CWE-787

## Recommendations



To address the vulnerabilities reported in Apple, we highly recommend that macOS Ventura, macOS Big Sur, and macOS Monterey users update their operating systems to the latest recommended versions as soon as possible. Apple has already resolved the issues of [macOS Ventura 13.3.1](#) and [Safari 16.4.1](#) of macOS Big Sur and macOS Monterey.



Be cautious when visiting websites that you are not familiar with or that seem suspicious. Attackers may use web-based attacks to exploit vulnerabilities in software. Use anti-malware software and keep it up-to-date. This can help to detect and block malicious software that may attempt to exploit vulnerabilities. Implementing hardening measures, such as firewalls, intrusion detection/prevention systems, and access controls can help to prevent unauthorized access to systems and sensitive data.

## Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0005</u></b> Defense Evasion
<b><u>TA0009</u></b> Collection	<b><u>TA0011</u></b> Command and Control	<b><u>TA0010</u></b> Exfiltration	<b><u>T1189</u></b> Drive-by Compromise
<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1102</u></b> Web Service	<b><u>T1005</u></b> Data from Local System	<b><u>T1048</u></b> Exfiltration Over Alternative Protocol
<b><u>T1547</u></b> Boot or Logon Autostart Execution	<b><u>T1547.006</u></b> Kernel Modules and Extensions	<b><u>T1014</u></b> Rootkit	

## Patch Links

<https://support.apple.com/en-us/HT213722>

<https://support.apple.com/en-us/HT213721>

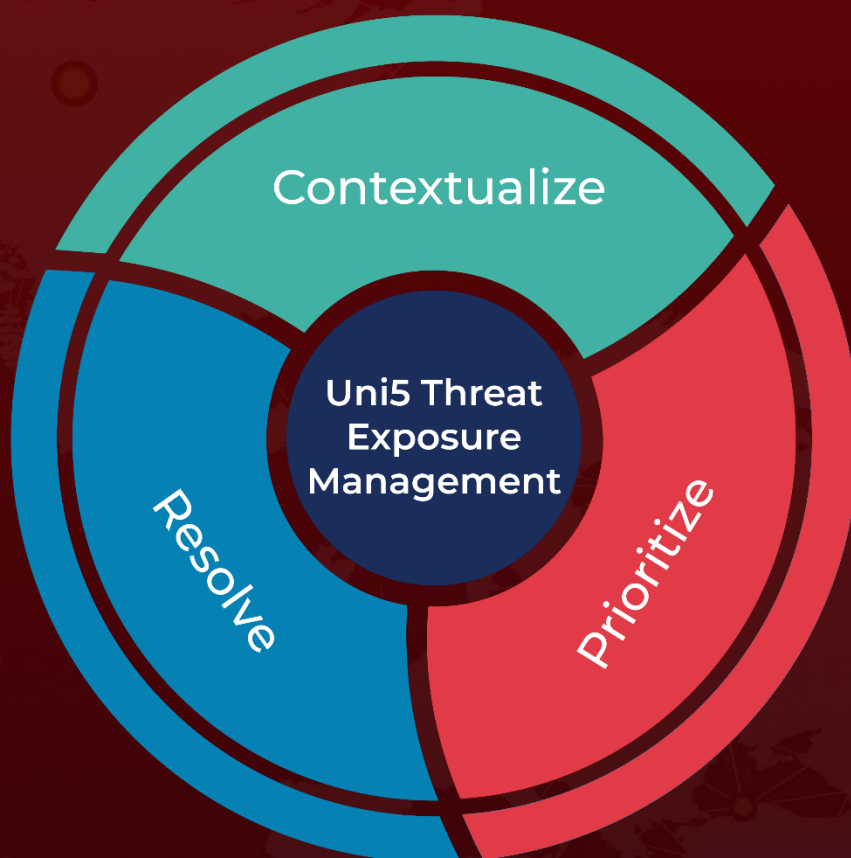
## References

<https://thehackernews.com/2023/04/apple-releases-updates-to-address-zero.html>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**April 11, 2023 • 2:00 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)