Hive Pro

THREAT ADVISORY

Zero-day vulnerability in WebKit affects Apple macOS

TA2022028

Threat Level RED

Publish Date – Feb 11, 2022

A third zero-day vulnerability has been identified since the latest zero-day bugs discovery in macOS Monterey in year 2022. This flaw impacts the WebKit component, which is a cross-platform web browser engine that is predominantly used in Safari.

This vulnerability tracked as CVE-2022-22620 exists due to a use-after-free error when processing HTML content in WebKit. The attacker can exploit this vulnerability by targeting users to visit a specially crafted web page. Once a user open the malicious web page, the attacker can remotely execute malicious code on the targeted system. In case of an attack where code injection and execution is successful, the behavior of the target machine is entirely dependent on the intended purpose of the injected code.

This vulnerability is been exploited in-the-wild and we suggest organizations to upgrade to macOS Monterey 12.2.1.

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
TA0002: Execution
T1204: User Execution
T1189: Drive-by Compromise
T1190: Exploit-public facing application
T1203: Exploitation for Client Execution
T1204.001: User Execution: Malicious Link

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-22620	macOS: 12.0 21A344, 12.0.1 21A559, 12.1 21C52, 12.2 21D49	cpe:2.3:o:apple:macos:12.0:21A334:*:*:*:*:*:*, cpe:2.3:o:apple:macos:12.0.1:21A559:*:*:*:*:*:*, cpe:2.3:o:apple:macos:12.1:21C52:*:*:*:*:*:*, cpe:2.3:o:apple:macos:12.2:21D49:*:*:*:*:*:*	A use after free vulnerability in the WebKit component	CWE-416

Patch Link

https://support.apple.com/en-us/HT213092

References

https://thehackernews.com/2022/02/apple-releases-ios-ipados-macos-updates.html