Hive Pro

THREAT ADVISORY

Two Vulnerabilities affecting Apple macOS exploited-in-the-wild

TA2022085

Threat Level RED

Publish Date – April 1, 2022

Two zero-day vulnerabilities were discovered in macOS Monterey versions prior to 12.3.1. These new issues bring the total number of zero-day vulnerabilities discovered in the Apple ecosystem to four.

CVE-2022-22674 is an out-of-bounds read vulnerability in the Intel Graphics Driver module that could allow a malicious actor to read kernel memory. CVE-2022-22675 is defined as an out-of-bounds write vulnerability in AppleAVD, an audio and video decoding component, that could allow an application to execute arbitrary code with kernel privileges.

This vulnerability is been exploited in-the-wild and we suggest organizations to upgrade to macOS Monterey 12.3.1.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
TA0040: Impact
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0009: Collection
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
T1190: Exploit Public-Facing Application
T1565: Data Manipulation
T1059: Command and Scripting Interpreter
T1574: Hijack Execution Flow
T1005: Data from Local System

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-22674	macOS Monterey version 12.3.1 and earlier	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	Out-of-bounds read issue in Intel Graphics Driver	CWE-125
CVE-2022-22675			Out-of-bounds write issue in AppleAVD	CWE-787

Patch Link

https://support.apple.com/en-us/HT213220

References

https://thehackernews.com/2022/03/apple-issues-patches-for-2-actively.html