Hive Pro

THREAT ADVISORY

Apple releases macOS Monterey 12.2 to fix multiple vulnerabilities

TA2022020

Threat Level RED

Publish Date – Jan 27, 2022

Apple has released a critical update for macOS Monterey that addresses two zero-day vulnerabilities with 11 other flaws.

One of the zero-day vulnerabilities is a memory corruption flaw in the IOMobileFrameBuffer component, which has been assigned CVE-2022-22587. An attacker could take advantage of this flaw by writing a specially designed application that allows them to run arbitrary code with kernel privileges. This is also been actively exploited in the wild

Another zero-day vulnerability is a cross-origin vulnerability exists due to incorrect implementation of the IndexDB API and has been assigned CVE-2022-22594. An attacker can exploit this input validation flaw using a malicious website to track users' online activity in the web browser and reveal their identity. This issue affects the 'WebKit Storage' component of the Safari and has been resolved in the latest version 15.3. This vulnerability, according to Apple, might be exploited in the wild.
The other Eleven flaws fixed in this update includes:

- CVE-2022-22587- A memory corruption vulnerability in the IOMobileFrameBuffer component
- CVE-2022-22594- A cross-origin vulnerability in the IndexDB API in the WebKit Storage component
- CVE-2022-22586- An out-of-bounds write vulnerability in the AMD Kernel component
- CVE-2022-22584- A memory corruption vulnerability in the ColorSync component
- CVE-2022-22578- A logic vulnerability in the Crash Reporter component
- CVE-2022-22585- A vulnerability existed within the path validation logic for symlinks in iCloud
- CVE-2022-22591- A memory corruption vulnerability in the Intel Graphics Driver component
- CVE-2022-22593- A buffer overflow vulnerability in the Kernel component
- CVE-2022-22579- An information disclosure vulnerability in the Model I/O component
- CVE-2022-22583- A permissions vulnerability in the PackageKit component
- CVE-2022-22589- A validation vulnerability in the WebKit component
- CVE-2022-22590- A use after free vulnerability in the WebKit component
- CVE-2022-22592- A logic vulnerability in the WebKit component

All these vulnerabilities have been fixed in macOS Monterey version 12.2

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-22587	macOS: 12.0 21A344, 12.0.1 21A559, 12.1 21C52	cpe:2.3:o:apple:macos:12.0:21A344:*:*:*:*:*:*:*, cpe:2.3:o:apple:macos:12.0.1:21A559:*:*:*:*:*:*:*, cpe:2.3:o:apple:macos:12.1:21C52:*:*:*:*:*:*:*	A memory corruption vulnerability in the IOMobileFrameBuffer component	CWE-119
CVE-2022-22594			A cross-origin vulnerability in the IndexDB API in the WebKit Storage component	CWE-200
CVE-2022-22586			An out-of-bounds write vulnerability in the AMD Kernel component	CWE-787
CVE-2022-22584			A memory corruption vulnerability in the ColorSync component	CWE-119

Hive Pro

THREAT ADVISORY

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-22578	macOS: 12.0 21A344, 12.0.1 21A559, 12.1 21C52	cpe:2.3:o:apple:macos:12.0:21A344:*:*:*:*:*:*:*, cpe:2.3:o:apple:macos:12.0.1:21A559:*:*:*:*:*:*:*, cpe:2.3:o:apple:macos:12.1:21C52:*:*:*:*:*:*:*	A logic vulnerability in the Crash Reporter component	CWE-264
CVE-2022-22585			A vulnerability existed within the path validation logic for symlinks in iCloud	CWE-59
CVE-2022-22591			A memory corruption vulnerability in the Intel Graphics Driver component	CWE-119
CVE-2022-22593			A buffer overflow vulnerability in the Kernel component	CWE-119
CVE-2022-22579			An information disclosure vulnerability in the Model I/O component	CWE-125
CVE-2022-22583			A permissions vulnerability in the PackageKit component	CWE-264
CVE-2022-22589			A validation vulnerability in the WebKit component	CWE-94
CVE-2022-22590			A use after free vulnerability in the WebKit component	CWE-416
CVE-2022-22592			A logic vulnerability in the WebKit component	CWE-254

Patch Link

https://support.apple.com/en-us/HT213054

References

https://www.cybersecurity-help.cz/vdb/SB2022012635
https://thehackernews.com/2022/01/apple-releases-ios-and-ipados-updates.html