Hive Pro

Threat Level

Amber

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft uncovers a macOS App Sandbox escape vulnerability

Date of Publication	Admiralty code	TA Number
July 15, 2022	A1	TA2022148

Summary

Microsoft has recently discovered a vulnerability in macOS that allows third parties to bypass sandbox restrictions and execute malicious commands.

CVE Table

CVE	NAME	PATCH
CVE-2022-26706	Permissions, Privileges, and Access Controls	✓

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1497** Virtualization/Sandbox Evasion	**TA0003** Persistence	**T1543** Create or Modify System Process

Technical Details

#1

The critical vulnerability CVE-2022-26706 can allow an attacker to take advantage of the security bypass and gain elevated privileges on the affected device and deploy malware. There are additional ways how the exploitation can affect its users, such as executing malicious code and installing additional payloads, damaging or compromising the application, etc.

#2

The vulnerability itself exists due to sandbox bypass in LaunchServices. However, the access issue has been addressed with additional sandbox restrictions on third-party applications. The fixed versions are macOS Big Sur 11.6.6 and macOS Monterey 12.4. macOS users are encouraged to install the security updates as soon as possible.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-26706	macOS: 11.0 20A2411 - 11.6.5 20G527	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	CWE- 264

Patch Links

https://support.apple.com/en-us/HT213256

https://support.apple.com/en-us/HT213257

References

https://www.microsoft.com/security/blog/2022/07/13/uncovering-a-macos-app-sandbox-escape-vulnerability-a-deep-dive-into-cve-2022-26706/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 15, 2022 • 1:10 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com