

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Apple Shortcuts' Secret Threat to Your Data

Date of Publication

February 26, 2023

Admiralty Code

A1

TA Number

TA2024075

Summary

First Seen: January 22, 2024

Affected Product: iOS and macOS

Impact: A security vulnerability, identified as CVE-2024-23204, has been found in Apple's Shortcuts application, allowing unauthorized access to sensitive information on devices bypassing TCC. The capability for users to export and share these shortcuts heightens the susceptibility to potential exploitation, as unsuspecting users may unwittingly import shortcuts with malicious intent. Ensure robust security measures are in place to safeguard against such vulnerabilities and protect your devices.

⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-23204	Apple Security features bypass Vulnerability	MacOS and iOS devices	✗	✗	✓

Vulnerability Details

#1

A security vulnerability has been discovered in Apple's Shortcuts app, presenting a significant risk as it enables a shortcut to access sensitive information on the device without explicit consent from users. This high-severity flaw, officially designated as CVE-2024-23204, was successfully addressed by Apple on January 22, 2024, through the deployment of updates for iOS 17.3, iPadOS 17.3, macOS Sonoma 14.3, and watchOS 10.3.

#2

The Shortcuts app, designed as an automation tool for macOS and iOS devices, empowers users to create personalized workflows to optimize tasks and enhance overall productivity. It acts as a platform for the distribution of shortcuts, with Apple hosting a gallery where users can explore and adopt automation workflows for task acceleration.

#3

Furthermore, Shortcuts can be exported and shared within the community, intensifying the potential impact of the vulnerability, as unsuspecting users may import shortcuts that exploit the CVE-2024-23204 flaw. The core of the issue lies in a specific shortcut action known as "Expand URL," capable of unraveling and refining URLs that have been shortened using services such as t.co or bit.ly, while simultaneously eliminating UTM tracking parameters. The vulnerability is on the brink of heightened exploitability due to the availability of exploitation techniques and the ease with which the attack can be executed.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-23204	macOS and iOS devices	cpe:2.3:o:apple:ipados: *:*:*:*:*:*:*: cpe:2.3:o:apple:iphone _os:*:*:*:*:*:*:*: cpe:2.3:o:apple:macos: *:*:*:*:*:*:*: cpe:2.3:o:apple:watcho s:*:*:*:*:*:*:*:	CWE-254

Recommendations



Apply Official Fixes Immediately: Apply the latest patches and updates for the Apple macOS and iOS devices to address the identified vulnerability (CVE-2024-23204).



Think Twice, Click Once: Exercise caution and restraint when importing shortcuts. Vigilance can prevent unauthorized access and potential data exposure.



Proactive Defense with Regular Checks: Make it a habit to regularly check for security updates and patches provided by Apple. Staying proactive in updating your devices adds an extra layer of defense against emerging vulnerabilities.



Review and Reevaluate Shortcuts: Take a moment to review and reevaluate the shortcuts you currently use. Deleting unnecessary or untrusted shortcuts minimizes potential risks associated with the vulnerability.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0007</u> Discovery	<u>TA0010</u> Exfiltration	<u>T1199</u> Trusted Relationship	<u>T1059</u> Command and Scripting Interpreter
<u>T1587.004</u> Exploits	<u>T1204</u> User Execution	<u>T1204.001</u> Malicious Link	<u>T1083</u> File and Directory Discovery
<u>T1048</u> Exfiltration Over Alternative Protocol			

Patch Details

The vulnerability was addressed in January with the release of iOS 17.3, iPadOS 17.3, and macOS Sonoma 14.3.

Links:

<https://support.apple.com/en-us/HT214059>

<https://support.apple.com/en-us/HT214060>

<https://support.apple.com/en-us/HT214061>

References

<https://www.bitdefender.com/blog/labs/details-on-apples-shortcuts-vulnerability-a-deep-dive-into-cve-2024-23204/>

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

February 26, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com