



# CVE-2022-42855

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-42855
<b>State</b>	PUBLIC
<b>Assigner</b>	product-security@apple.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-15 19:15:00 UTC
<b>Updated</b>	2023-06-06 23:15:00 UTC
<b>Description</b>	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.2, macOS Monterey 12.6.2, m

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Ipados</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	13.0	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Tvos</a>	All	All	All	All

## References

Reference	Source	Link	Tags
libCoreEntitlements CGContextQuery Arbitrary Entitlement Returns ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
About the security content of watchOS 9.2 - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>	
Full Disclosure: APPLE-SA-2022-12-13-2 iOS 15.7.2 and iPadOS 15.7.2	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
Full Disclosure: APPLE-SA-2022-12-13-1 iOS 16.2 and iPadOS 16.2	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
About the security content of macOS Monterey 12.6.2 - Apple Support	MISC	<a href="https://support.apple.com">support.apple.com</a>	
Full Disclosure: APPLE-SA-2022-12-13-5 macOS Monterey 12.6.2	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
About the security content of tvOS 16.2 - Apple Support	MISC	<a href="https://support.apple.com">support.apple.com</a>	
About the security content of macOS Ventura 13.1 - Apple Support	MISC	<a href="https://support.apple.com">support.apple.com</a>	
Full Disclosure: APPLE-SA-2022-12-13-4 macOS Ventura 13.1	FULLDISC	<a href="https://seclists.org">seclists.org</a>	

20221220 APPLE-SA-2022-12-13-7 tvOS 16.2	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
About the security content of iOS 16.2 and iPadOS 16.2 - Apple Support	MISC	<a href="https://support.apple.com">support.apple.com</a>	
About the security content of iOS 15.7.2 and iPadOS 15.7.2 - Apple Support	MISC	<a href="https://support.apple.com">support.apple.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ana

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [377831](#) Apple macOS Monterey 12.6.2 Not Installed (HT213533)
- [377838](#) Apple macOS Ventura 13.1 Not Installed (HT213532)
- [610455](#) Apple iOS 15.7.2 and iPadOS 15.7.2 Security Update Missing
- [610456](#) Apple iOS 16.2 and iPadOS 16.2 Security Update Missing

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)