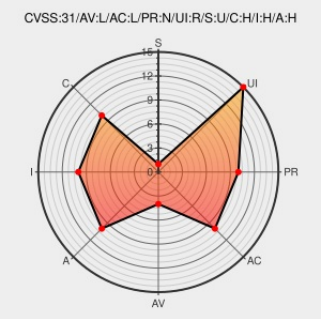
CVE-2022-26757

Published on: Not Yet Published

Last Modified on: 01/31/2023 05:42:00 PM UTC

CVE-2022-26757

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ipados from Apple contain the following vulnerability:

A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, Security Update 2022-004 Catalina, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.4. An application may be able to execute arbitrary code with kernel privileges.

CVE-2022-26757 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
About the security content of Security Update 2022-004 Catalina - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213255
About the security content of tvOS 15.5 - Apple	support.apple.com	MISC support.apple.com/en-us/HT213254

Support	text/html	
About the security content of watchOS 8.6 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213253
About the security content of iOS 15.5 and iPadOS 15.5 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213258
About the security content of macOS Big Sur 11.6.6 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213256
XNU Flow Divert Race Condition Use-After-Free ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/167517/XNU-Flow-Divert-Race-Condition-Use-After-Free.html
About the security content of macOS Monterey 12.4 - Apple Support	support.apple.com text/html	MISC support.apple.com/en-us/HT213257

Related QID Numbers

376607 Apple macOS Security Update 2022-004 Catalina (HT213255)

376608 Apple MacOS Big Sur 11.6.6 Not Installed (HT213256)

376612 Apple macOS Monterey 12.4 Not Installed (HT213257)

610416 Apple iOS 15.5 and iPadOS 15.5 Security Update Missing (HT213258)

Exploit/POC from Github

Flow Divert Race Condition Bug (CVE-2022-26757) discovered by @nedwill

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Macos	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.15.7	-	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2020-001	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-001	All	All
Operating	Apple	Mac Os X	10.15.7	security_update_2021-002	All	All

System						
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-003	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-004	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-005	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-006	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-007	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-008	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-001	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-002	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-003	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:-:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2020-001:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-001:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-002:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-003:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-004:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-005:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-006:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-007:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-008:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2022-001:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2022-002:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2022-003:*:*:*:*:*:*:

cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-26757 : A use after free issue was addressed with improved memory management. This issue is fixed in tvOS… twitter.com/i/web/status/1…	2022-05-26 20:12:23
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-17 13:11:14
/r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-18 14:59:44
/r/netcve	CVE-2022-26757	2022-05-26 21:38:59

← Previous ID

Next ID→