



# CVE-2022-26757

Published on: Not Yet Published

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

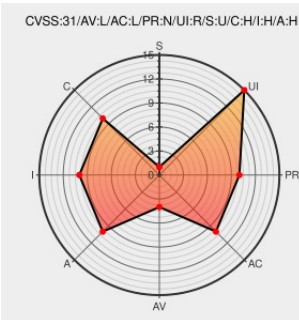
## CVE-2022-26757

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
<b>LOCAL</b>	<b>LOW</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>COMPLETE</b>	<b>COMPLETE</b>	<b>COMPLETE</b>

## CVE References

Description	Tags	Link
About the security content of Security Update 2022-004 Catalina - Apple Support	<a href="#">support.apple.com</a> <a href="#">text/html</a>	MISC <a href="https://support.apple.com/en-us/HT213255">support.apple.com/en-us/HT213255</a>
About the security content of tvOS 15.5 - Apple	<a href="#">support.apple.com</a>	MISC <a href="https://support.apple.com/en-us/HT213254">support.apple.com/en-us/HT213254</a>

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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

### 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	<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="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	-	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2020-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-05-26 20:12:23
 /r/k12cybersecurity	<a href="#">MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW</a>	2022-05-17 13:11:14
 /r/k12cybersecurity	<a href="#">UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW</a>	2022-05-18 14:59:44
 /r/netcve	<a href="#">CVE-2022-26757</a>	2022-05-26 21:38:59

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)