



# CVE-2024-44213

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

## Summary

<b>CVE</b>	CVE-2024-44213
<b>State</b>	PUBLISHED
<b>Assigner</b>	apple
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-10-28 21:15:06 UTC
<b>Updated</b>	2026-04-02 19:18:22 UTC
<b>Description</b>	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in mac

## Risk And Classification

**Primary CVSS:** v3.1 5.9 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

**Problem Types:** NVD-CWE-noinfo | CWE-922 | An attacker in a privileged network position may be able to leak sensitive user information | CWE-922 CWE-922 Insecure Storage of Sensitive Information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apple	MacOS	affected 13.7.1 custom	Not specified
CNA	Apple	MacOS	affected 14.7.1 custom	Not specified
CNA	Apple	MacOS	affected 15.1 custom	Not specified
ADP	Apple	Macos	affected 14.7 custom	Not specified
ADP	Apple	Macos	affected 13.7 custom	Not specified

### References

Reference	Source	Link	Tags
seclists.org/fulldisclosure/2024/Oct/12	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	
support.apple.com/en-us/121568	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
seclists.org/fulldisclosure/2024/Oct/13	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	
seclists.org/fulldisclosure/2024/Oct/11	af854a3a-2127-422b-91ae-364da2661108	<a href="https://seclists.org">seclists.org</a>	
support.apple.com/en-us/121564	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	
support.apple.com/en-us/121570	product-security@apple.com	<a href="https://support.apple.com">support.apple.com</a>	Release Notes, Vendor Advisory
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, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**