



CVE-2023-40401

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-40401 |
| State | PUBLIC |
| Assigner | product-security@apple.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-10-25 19:15:00 UTC |
| Updated | 2023-11-02 19:43:00 UTC |
| Description | The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.6.1. An attacker may |

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

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

References

| Reference | Source | Link | Tags |
|--|---------|-----------------------------------|---------------------|
| Full Disclosure: APPLE-SA-10-25-2023-5 macOS Ventura 13.6.1 | MISC | seclists.org | |
| About the security content of macOS Ventura 13.6.1 - Apple Support | MISC | support.apple.com | |
| About the security content of macOS Ventura 13.6.1 - Apple Support | MISC | support.apple.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378970](#) Apple macOS Ventura 13.6.1 Not Installed (HT213985)

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](#)