



# CVE-2020-19185

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2020-19185   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2023-08-22 19:15:00 UTC  |
| <b>Updated</b>         | 2023-12-13 01:15:00 UTC  |
| <b>Description</b>     | Buffer Overflow vulnerability in one_one_mapping function in progs/dump_entry.c:1373 in ncurses 6.1 allows remote attack |

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                                   | Version | Update | Edition | Language |
|-------------|------------------------|---|---------|--------|---------|----------|
| Application | <a href="#">Gnu</a>    | <a href="#">Ncurses</a>                   | 6.1     | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Active Iq Unified Manager</a> | -       | All    | All     | All      |

## References

| Reference  | Source  | Link  | Tags           |
|--|---------|---|----------------|
| About the security content of macOS Ventura 13.6.3 - Apple Support                   |         | <a href="https://support.apple.com">support.apple.com</a>     |                |
| August 2023 GNU Ncurses Vulnerabilities in NetApp Products   NetApp Product Security | CONFIRM | <a href="https://security.netapp.com">security.netapp.com</a> |                |
| Full Disclosure: APPLE-SA-12-11-2023-6 macOS Monterey 12.7.2                         |         | <a href="https://seclists.org">seclists.org</a>               |                |
| About the security content of macOS Sonoma 14.2 - Apple Support                      |         | <a href="https://support.apple.com">support.apple.com</a>     |                |
| Full Disclosure: APPLE-SA-12-11-2023-5 macOS Ventura 13.6.3                          |         | <a href="https://seclists.org">seclists.org</a>               |                |
| About the security content of macOS Monterey 12.7.2 - Apple Support                  |         | <a href="https://support.apple.com">support.apple.com</a>     |                |
| Full Disclosure: APPLE-SA-12-11-2023-4 macOS Sonoma 14.2                             |         | <a href="https://seclists.org">seclists.org</a>               |                |
| heap-buffer-overflow, one_one_mapping, progs/dump_entry.c:1373, ncurses 6.1          | MISC    | <a href="https://github.com">github.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, and |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[379124](#) Apple macOS Ventura 13.6.3 Not Installed (HT214038)

[379125](#) Apple macOS Sonoma 14.2 Not Installed (HT214036)

[379126](#) Apple macOS Monterey 12.7.2 Not Installed (HT214037)

© [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](#) 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](#)