



# CVE-1999-0475

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-1999-0475  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 1999-04-05 04:00:00 UTC  |
| <b>Updated</b>         | 2022-08-17 08:15:00 UTC  |
| <b>Description</b>     | A race condition in how procmail handles .procmailrc files allows a local user to read arbitrary files available to the user who |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                   | Product                  | Version | Update | Edition | Language |
|-------------|--------------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Procmail</a> | <a href="#">Procmail</a> | All     | All    | All     | All      |
| Application | <a href="#">Procmail</a> | <a href="#">Procmail</a> | All     | All    | All     | All      |

## References

| Reference                | Source  | Link  | Tags                |
|--------------------------|---------|---|---------------------|
| IBM X-Force Exchange     | MISC    | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.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, analysis |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[901863](#) Common Base Linux Mariner (CBL-Mariner) Security Update for procmail (7330)

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](#)**