



# CVE-2023-4016

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-4016
<b>State</b>	PUBLIC
<b>Assigner</b>	trelixpsirt@trelix.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-02 05:15:00 UTC
<b>Updated</b>	2023-08-21 03:15:00 UTC
<b>Description</b>	Under some circumstances, this weakness allows a user who has access to run the "ps" utility on a machine, the ability to v

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Procps Project</a>	<a href="#">Procps</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 38 Update: procps-ng-3.3.17-11.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
procps-ng / procps · GitLab	MISC	<a href="https://gitlab.com">gitlab.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[161069](#) Oracle Enterprise Linux Security Update for procps-ng (ELSA-2023-6705)

[161168](#) Oracle Enterprise Linux Security Update for procps-ng (ELSA-2023-7187)

[199898](#) Ubuntu Security Notification for procps-ng Vulnerability (USN-6477-1)

[242356](#) Red Hat Update for procps-ng (RHSA-2023:6705)

242459 Red Hat Update for procps-ng (RHSA-2023:7187)
284430 Fedora Security Update for procps (FEDORA-2023-30c3ca07eb)
379251 Alibaba Cloud Linux Security Update for procps-ng (ALINUX3-SA-2024:0003)
503483 Alpine Linux Security Update for procps
503484 Alpine Linux Security Update for procps
503485 Alpine Linux Security Update for procps
505923 Alpine Linux Security Update for procps-ng
673453 EulerOS Security Update for procps-ng (EulerOS-SA-2023-3041)
673517 EulerOS Security Update for procps-ng (EulerOS-SA-2023-3226)
673607 EulerOS Security Update for procps-ng (EulerOS-SA-2023-3147)
673642 EulerOS Security Update for procps-ng (EulerOS-SA-2024-1159)
673741 EulerOS Security Update for procps-ng (EulerOS-SA-2023-3018)
673829 EulerOS Security Update for procps-ng (EulerOS-SA-2023-2886)
673895 EulerOS Security Update for procps-ng (EulerOS-SA-2023-2905)
673974 EulerOS Security Update for procps-ng (EulerOS-SA-2023-3191)
941410 AlmaLinux Security Update for procps-ng (ALSA-2023:6705)
941432 AlmaLinux Security Update for procps-ng (ALSA-2023:7187)
961076 Rocky Linux Security Update for procps-ng (RLSA-2023:7187)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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