



# CVE-2023-33204

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

## Summary

<b>CVE</b>	CVE-2023-33204
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-18 08:15:00 UTC
<b>Updated</b>	2023-11-07 04:14:00 UTC
<b>Description</b>	sysstat through 12.7.2 allows a multiplication integer overflow in check_overflow in common.c. NOTE: this issue exists beca

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Application	<a href="#">Sysstat Project</a>	<a href="#">Sysstat</a>	All	All	All	All

## References

Reference	Source	Link
Fix an overflow which is still possible for some values. by pkopylov · Pull Request #360 · sysstat/sysstat · GitHub	MISC	<a href="#">github.com</a>
[SECURITY] Fedora 37 Update: sysstat-12.6.2-2.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 38 Update: sysstat-12.7.4-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] [DLA 3434-1] sysstat security update	MLIST	<a href="#">lists.debian.org</a>
[SECURITY] Fedora 38 Update: sysstat-12.7.4-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 37 Update: sysstat-12.6.2-2.fc37 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

161075 Oracle Enterprise Linux Security Update for sysstat (ELSA-2023-6569)
161136 Oracle Enterprise Linux Security Update for sysstat (ELSA-2023-7010)
181805 Debian Security Update for sysstat (DLA 3434-1)
199402 Ubuntu Security Notification for Sysstat Vulnerabilities (USN-6145-1)
242311 Red Hat Update for sysstat (RHSA-2023:6569)
242450 Red Hat Update for sysstat (RHSA-2023:7010)
284124 Fedora Security Update for sysstat (FEDORA-2023-ac947ec260)
284324 Fedora Security Update for sysstat (FEDORA-2023-4706cef256)
355385 Amazon Linux Security Advisory for sysstat : ALAS2-2023-2068
355405 Amazon Linux Security Advisory for sysstat : ALAS2023-2023-191
379640 Alibaba Cloud Linux Security Update for sysstat (ALINUX3-SA-2024:0042)
673228 EulerOS Security Update for sysstat (EulerOS-SA-2023-2370)
673241 EulerOS Security Update for sysstat (EulerOS-SA-2023-2396)
673289 EulerOS Security Update for sysstat (EulerOS-SA-2023-2629)
673301 EulerOS Security Update for sysstat (EulerOS-SA-2023-2599)
673455 EulerOS Security Update for sysstat (EulerOS-SA-2023-2713)
673843 EulerOS Security Update for sysstat (EulerOS-SA-2023-3161)
674044 EulerOS Security Update for sysstat (EulerOS-SA-2023-2671)
906938 Common Base Linux Mariner (CBL-Mariner) Security Update for sysstat (26784-1)
941398 AlmaLinux Security Update for sysstat (ALSA-2023:6569)
941472 AlmaLinux Security Update for sysstat (ALSA-2023:7010)

© [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](#)