



CVE-2022-26530

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

Summary

CVE	CVE-2022-26530
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-03 23:15:00 UTC
Updated	2022-04-19 03:08:00 UTC
Description	swaylock before 1.6 allows attackers to trigger a crash and achieve unlocked access to a Wayland compositor.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Swayvm	Swaylock	All	All	All	All
Application	Swaywm	Swaylock	All	All	All	All

References

Reference	Source	Link	Tags
2066596 – (CVE-2022-26530) CVE-2022-26530 swaylock: lock screen bypasses	CONFIRM	bugzilla.redhat.com	
Add support for ext-session-lock-v1 · swaywm/swaylock@1d1c75b · GitHub	MISC	github.com	
Add support for ext-session-lock-v1 by emersion · Pull Request #219 · swaywm/swaylock · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[184641](#) Debian Security Update for swaylock (CVE-2022-26530)

[282535](#) Fedora Security Update for swaylock (FEDORA-2022-194c3da292)

[502367](#) Alpine Linux Security Update for swaylock

© [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](#)