



# CVE-2021-26937

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

## Summary

<b>CVE</b>	CVE-2021-26937
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-09 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:31:00 UTC
<b>Description</b>	encoding.c in GNU Screen through 4.8.0 allows remote attackers to cause a denial of service (invalid write access and app

## Risk And Classification

### Problem Types: CWE-88

## 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="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Screen</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 32 Update: screen-4.8.0-5.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Mailir
GNU Screen: User-assisted execution of arbitrary code (GLSA 202105-11) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
[SECURITY] Fedora 33 Update: screen-4.8.0-5.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Mailir
[screen-devel] [bug #60030] Screen segfaults by displaying some UTF-8 ch	MISC	<a href="https://lists.gnu.org">lists.gnu.org</a>	Explo
[SECURITY] [DLA 2570-1] screen security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailir

[SECURITY] Fedora 32 Update: screen-4.8.0-5.fc32 - package-announce - Fedora Mailing-Lists			<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Index of ftp.gnu.org/gnu/screen	MISC		<a href="https://ftp.gnu.org">ftp.gnu.org</a>	Produ
[SECURITY] Fedora 33 Update: screen-4.8.0-5.fc33 - package-announce - Fedora Mailing-Lists			<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Debian -- Security Information -- DSA-4861-1 screen	DEBIAN		<a href="https://www.debian.org">www.debian.org</a>	Third
oss-security - Re: screen crash processing combining characters	MLIST		<a href="https://www.openwall.com">www.openwall.com</a>	Explo
oss-security - screen crash processing combining characters	MISC		<a href="https://www.openwall.com">www.openwall.com</a>	Explo
CVE Program record	CVE.ORG		<a href="https://www.cve.org">www.cve.org</a>	canor
NVD vulnerability detail	NVD		<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canor

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [179498](#) Debian Security Update for screen (CVE-2021-26937)
- [240450](#) Red Hat Update for screen (RHSA-2022:1074)
- [257075](#) CentOS Security Update for screen (CESA-2021:0742)
- [281598](#) Fedora Security Update for screen (FEDORA-2021-5e9894a0c5)
- [281599](#) Fedora Security Update for screen (FEDORA-2021-9107eeb95c)
- [296067](#) Oracle Solaris 11.4 Support Repository Update (SRU) 33.94.0 Missing (CPUAPR2021)
- [352259](#) Amazon Linux Security Advisory for screen: ALAS2-2021-1623
- [352261](#) Amazon Linux Security Advisory for screen: ALAS-2021-1492
- [377067](#) Alibaba Cloud Linux Security Update for screen (ALINUX2-SA-2021:0012)
- [500639](#) Alpine Linux Security Update for screen
- [501494](#) Alpine Linux Security Update for screen
- [504404](#) Alpine Linux Security Update for screen
- [670227](#) EulerOS Security Update for screen (EulerOS-SA-2021-1848)
- [670311](#) EulerOS Security Update for screen (EulerOS-SA-2021-1913)
- [670336](#) EulerOS Security Update for screen (EulerOS-SA-2021-1888)
- [670432](#) EulerOS Security Update for screen (EulerOS-SA-2021-2068)
- [670443](#) EulerOS Security Update for screen (EulerOS-SA-2021-2057)
- [670689](#) EulerOS Security Update for screen (EulerOS-SA-2021-2447)
- [670879](#) EulerOS Security Update for screen (EulerOS-SA-2021-1888)

670929 EulerOS Security Update for screen (EulerOS-SA-2021-2068)

710104 Gentoo Linux GNU Screen User-assisted execution of arbitrary code vulnerability (GLSA 202105-11)

750354 OpenSUSE Security Update for screen (openSUSE-SU-2021:0304-1)

901416 Common Base Linux Mariner (CBL-Mariner) Security Update for screen (7356)

908078 Common Base Linux Mariner (CBL-Mariner) Security Update for screen (7356-1)

© [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](#)**