



CVE-2020-35573

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

Summary

CVE	CVE-2020-35573
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-20 05:15:00 UTC
Updated	2022-04-26 16:12:00 UTC
Description	srs2.c in PostSRSD before 1.10 allows remote attackers to cause a denial of service (CPU consumption) via a long timestamp

Risk And Classification

Problem Types: CWE-834

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Postersrd Prject	Postersrd	All	All	All	All
Application	Postersrd Prject	Postersrd	All	All	All	All
Application	Postersrd Project	Postersrd	All	All	All	All

References

Reference	Source	Link
PostSRSD: Denial of service (GLSA 202107-08) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] [DLA 2502-1] postersrd security update	MLIST	lists.debian.org
SECURITY: Fix potential denial of service attack against PostSRSD · roehling/postersrd@4733fb1 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501225 Alpine Linux Security Update for postsrcsd
690358 Free Berkeley Software Distribution (FreeBSD) Security Update for postsrcsd (eb2845c4-43ce-11eb-aba5-00a09858faf5)
710068 Gentoo Linux PostSRSD Denial of service (GLSA 202107-08)
750234 OpenSUSE Security Update for postsrcsd (openSUSE-SU-2021:0646-1)

© [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](#).

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

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