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 timestar

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	Postsrsd Prject	Postsrsd	All	All	All	All
Application	Postsrsd Prject	Postsrsd	All	All	All	All
Application	Postsrsd Project	Postsrsd	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] postsrsd security update	MLIST	lists.debian.org
SECURITY: Fix potential denial of service attack against PostSRSd · roehling/postsrsd@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 postsrsd

690358 Free Berkeley Software Distribution (FreeBSD) Security Update for postsrsd (eb2845c4-43ce-11eb-aba5-00a09858faf5)

710068 Gentoo Linux PostSRSd Denial of service (GLSA 202107-08)

750234 OpenSUSE Security Update for postsrsd (openSUSE-SU-2021:0646-1)