CVE-2021-33912

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-33912
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-19 18:15:00 UTC
Updated	2024-01-15 17:15:00 UTC
Description	libspf2 before 1.2.11 has a four-byte heap-based buffer overflow that might allow remote attackers to execute arbitrary code

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libspf2 Project	Libspf2	All	All	All	All

References

Reference	Source	Link
CVE-2021-33912 and CVE-2021-33913: Heap overflows in email validation library LibSPF2 | Nathaniel Bennett	MISC	nathanielbenne
GitHub - shevek/libspf2 at 8131fe140704eaae695e76b5cd09e39bd1dd220b	MISC	github.com
libspf2: Multiple vulnerabilities (GLSA 202401-22) — Gentoo security		security.gentoo
[SECURITY] [DLA 2890-1] libspf2 security update	MLIST	lists.debian.org
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

179014 Debian Security Update for libspf2 (DLA 2890-1)

179776 Debian Security Update for libspf2 (CVE-2021-33912)

200049 Ubuntu Security Notification for Libspf2 Vulnerabilities (USN-6584-1)

200128 Ubuntu Security Notification for Libspf2 Vulnerabilities (USN-6584-2)

502222 Alpine Linux Security Update for libspf2

503678 Alpine Linux Security Update for libspf2

505886 Alpine Linux Security Update for libspf2

710839 Gentoo Linux libspf2 Multiple Vulnerabilities (GLSA 202401-22)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**