CVE-2023-42118

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

Summary

CVE	CVE-2023-42118
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	Unknown
Updated	2023-09-06 22:06:12 UTC
Description	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 284595 Fedora Security Update for libspf2 (FEDORA-2023-ae340c92ea)
- 284596 Fedora Security Update for libspf2 (FEDORA-2023-7f01e967ad)
- 285229 Fedora Security Update for libspf2 (FEDORA-2023-b317dd9220)
- 503368 Alpine Linux Security Update for libspf2
- 505887 Alpine Linux Security Update for libspf2
- 691319 Free Berkeley Software Distribution (FreeBSD) Security Update for libspf2 (915855ad-283d-4597-b01e-e0bf611db78b)

© 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 registred 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**