



CVE-2021-20314

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

Summary

CVE	CVE-2021-20314
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-12 15:15:00 UTC
Updated	2024-01-15 17:15:00 UTC
Description	Stack buffer overflow in libspf2 versions below 1.2.11 when processing certain SPF macros can lead to Denial of service ar

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Libspf2	Libspf2	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: libspf2-1.2.11-1.20210922git4915c308.fc35 - package-announce - Fedora Mailing-Lists	MISC	lists.f
[SECURITY] Fedora 35 Update: libspf2-1.2.11-1.20210922git4915c308.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
[SECURITY] Fedora 33 Update: libspf2-1.2.11-1.20210922git4915c308.fc33 - package-announce - Fedora Mailing-Lists	MISC	lists.f
[SECURITY] Fedora 34 Update: libspf2-1.2.11-1.20210922git4915c308.fc34 - package-announce - Fedora Mailing-Lists	MISC	lists.f
[SECURITY] Fedora 34 Update: libspf2-1.2.11-1.20210922git4915c308.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
[SECURITY] Fedora 33 Update: libspf2-1.2.11-1.20210922git4915c308.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
1993070 – (CVE-2021-20314) CVE-2021-20314 libspf2: stack buffer overflow when processing SPF explanation macros	MISC	bugzi
libspf2: Multiple vulnerabilities (GLSA 202401-22) — Gentoo security		secur
CVE Program record	CVE.ORG	www.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178753	Debian Security Update for libspf2 (DSA 4955-1)
178756	Debian Security Update for libspf2 (DLA 2739-1)
179606	Debian Security Update for libspf2 (CVE-2021-20314)
200049	Ubuntu Security Notification for Libspf2 Vulnerabilities (USN-6584-1)
281944	Fedora Security Update for libspf2 (FEDORA-2021-994751581f)
281945	Fedora Security Update for libspf2 (FEDORA-2021-044be3d54e)
500317	Alpine Linux Security Update for libspf2
504084	Alpine Linux Security Update for libspf2
710839	Gentoo Linux libspf2 Multiple Vulnerabilities (GLSA 202401-22)
751051	OpenSUSE Security Update for libspf2 (openSUSE-SU-2021:1187-1)

© [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](#)