



Red Hat 製品エラータ RHSA-2026:1948 - Security Advisory

RHSA-2026:1948 - Security Advisory

発行日: 2026-02-04 更新日: 2026-02-04

[概要](#)[更新パッケージ](#)

概要

Important: libsoup security update

タイプ/重大度

Security Advisory: Important

Red Hat Lightspeed patch analysis

このアドバイザリーの影響を受けるシステムを特定し、修正します。

[影響を受けるシステムの表示](#)

トピック

An update for libsoup is now available for Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions and Red Hat Enterprise Linux 8.8 Telecommunications Update Service.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

説明

The libsoup packages provide an HTTP client and server library for GNOME.

Security Fix(es):

- libsoup: Signed to Unsigned Conversion Error Leading to Stack-Based Buffer Overflow in libsoup NTLM Authentication (CVE-2026-0719)
- libsoup: Stack-Based Buffer Overflow in libsoup Multipart Response Parsingmultipart HTTP response (CVE-2026-1761)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

解決策



For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 



影響を受ける製品

- Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64
- Red Hat Enterprise Linux Server - TUS 8.8 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64

修正

- BZ - 2427906  - CVE-2026-0719 libsoup: Signed to Unsigned Conversion Error Leading to Stack-Based Buffer Overflow in libsoup NTLM Authentication
- BZ - 2435961  - CVE-2026-1761 libsoup: Stack-Based Buffer Overflow in libsoup Multipart Response Parsingmultipart HTTP response

CVE

- CVE-2026-0719 
- CVE-2026-1761 

参考資料

- <https://access.redhat.com/security/updates/classification/#important> 

Red Hat のセキュリティーに関する連絡先は secalert@redhat.com です。連絡先の詳細は <https://access.redhat.com/security/team/contact/> をご覧ください。



Quick Links 

Help 

Site Info 

Related Sites 

 All systems operational



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Opt-Out Rights](#)