CVE-

VEX

Public on

Last modi

cription

ements

Descri

A flaw in he last occurren , so this mismatcl kend interprets it as destined for another host. This discrepancy enables request-smuggling style attacks, cache poisoning, or bypassing host-based access controls when an attacker supplies duplicate Host headers.

Statement

This vulnerability is rated Important for Red Hat products that utilize libsoup in environments where applications are exposed via a front proxy. The flaw arises from a discrepancy in how libsoup processes duplicate Host: headers (last-value wins) compared to many proxies (first-value wins). This mismatch

can lead to virtual-host confusion, enabling attackers to bypass host-based access controls or perform cache poisoning. Systems where libsoup applications are directly accessible without an intervening proxy are not affected by this specific issue.

Mitigation

Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Additional information

- Bugzilla 2421349: libsoup: libsoup: Duplicate Host Header Handling Causes Host-Parsing Discrepancy (First- vs Last-Value Wins)
- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

External references

- https://www.cve.org/CVERecord?id=CVE-2025-14523
- https://nvd.nist.gov/vuln/detail/CVE-2025-14523

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata

Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	libsoup3
State	Fixed
Justification	None
Errata	RHSA-2026:0423

Release Date	January 12, 2026
Products / Services	Red Hat Enterprise Linux 10.0 Extended Update Support
Components	libsoup3
State	Fixed
Justification	None
Errata	RHSA-2026:0836
Release Date	January 20, 2026
Products / Services	Red Hat Enterprise Linux 7 Extended Lifecycle Support

1-10 of 27

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	8.2	N/A
Attack Vector	Network	N/A

	Red Hat	NVD
Attack Complexity	Low	N/A
Privileges Required	None	N/A
User Interaction	None	N/A
Scope	Unchanged	N/A
Confidentiality Impact	Low	N/A
Integrity Impact	High	N/A
Availability Impact	None	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

Acknowledgements

Red Hat would like to thank Ky0toFu and Sovereign Tech Resilience program for reporting this issue.

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors? >
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability? >
- What can I do if my product is listed as "Will not fix"? >
- What can I do if my product is listed as "Fix deferred"? >
- What is a mitigation? >

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

My product is listed as "Out of Support Scope". What does this mean?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: January 12, 2026 at 1:39:58 AM UTC