Cross-Site Scripting (XSS) in DeepL Chrome Extension

Moderate **kai-deepl** published **GHSA-4x2r-q3p9-xhx4** on Jan 23

Package

DeepL Chrome Extension (Chrome Extension)

Affected versions

v1.22.0, v1.22.1, v1.22.2, v.1.23.0

Patched versions

v1.24.0

Description

A cross-site scripting vulnerability (XSS) was introduced in the DeepL Chrome extension with version v1.22.0 due to improper neutralization of input during web page generation. Incomplete fixes were released with versions v1.22.2 and v1.23.0. A complete fix was released with version 1.24.0.

The extension failed to properly sanitize user-controlled input (such as search queries or page content) before rendering it into the DOM. This allows for the execution of arbitrary JavaScript in the context of the user's browser.

Severity

Moderate 5.1 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	Active

Vulnerable System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CVE ID

CVE-2026-40451

Weaknesses

- CWE-79
- CWE-80

Credits

halilkirazkaya Reporter