



Published:2026/04/22 Last Updated:2026/04/22

JVN#37524771

DeepL Chrome browser extension vulnerable to cross-site scripting

Overview

DeepL Chrome browser extension contains a cross-site scripting vulnerability.

Products Affected

- DeepL Chrome browser extension from v1.22.0 to v.1.23.0

DeepL web application is not affected by the vulnerability.

Description

DeepL Chrome browser extension contains the following vulnerability.

- **Cross-site scripting (CWE-79)**
 - 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 Base Score 5.1
 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score 6.1
 - CVE-2026-40451

Impact

- An arbitrary script may be executed on a user's browser, and malicious HTML may be injected into web pages viewed by the user.

Solution

Update the Software

Update the software to the latest version according to the information provided by the developer.

Vendor Status

Vendor Link

DeepL [Cross-Site Scripting \(XSS\) in DeepL Chrome Extension](#)

References

JVN

[HOME](#)[What is JVN ?](#)[Instructions](#)[List of Vulnerability Report](#)[VN_JP](#)[VN_JP\(Unreachable\)](#)[VN_VU](#)[TA](#)[TRnotes](#)[JVN iPedia](#)[MyJVN](#)[JVNJS/RSS](#)[Vendor List](#)[List of unreachable developers](#)[Contact](#)

JPCERT/CC Addendum

Vulnerability Analysis by JPCERT/CC

Credit

This vulnerability was reported by the researchers below and JPCERT/CC coordinated with the developer.

Junki Yuasa of Cybozu, Inc. reported this vulnerability to JPCERT/CC.

Keitaro Yamazaki of GMO Cybersecurity by Ierae reported this vulnerability to IPA under Information Security Early Warning Partnership.

Other Information

JPCERT Alert

JPCERT Reports

CERT Advisory

CPNI Advisory

TRnotes

CVE [CVE-2026-40451](#)

JVN iPedia [JVND-2026-000060](#)

Copyright (c) 2000-2026 JPCERT/CC and IPA. All rights reserved.